

E-BOOK

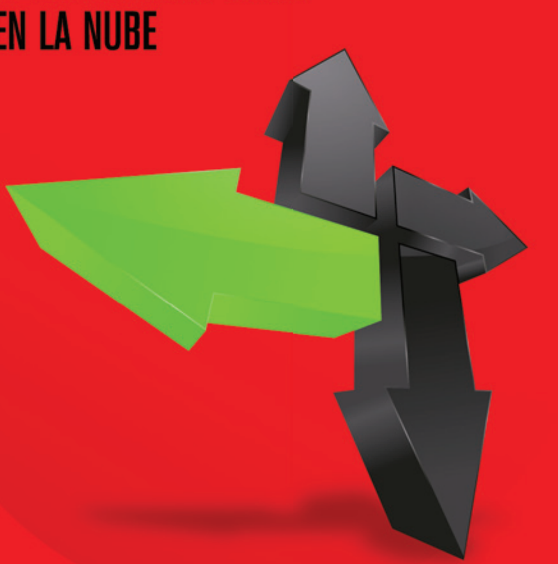
Técnico en
REDES
&SEGURIDAD

7

SOLUCIÓN DE PROBLEMAS

CONCEPTOS, SERVICIOS Y HERRAMIENTAS CLAVE SOBRE LA COMPUTACIÓN EN LA NUBE

- SERVICIOS MÁS CONOCIDOS
- CARACTERÍSTICAS
- USO PERSONAL
- DISTINTOS TIPOS DE NUBE







7

SOLUCIÓN DE PROBLEMAS





TÍTULO: Solución de problemas
COLECCIÓN: Pocket Users

Primera edición realizada en abril de MMXIII.

EISBN 978-987-1949-06-9

González Rodríguez, Gilberto
Solución de problemas. - 1a ed. - Buenos Aires : Fox Andina, 2013.
E-Book - (Pocket users 32)
ISBN 978-987-1949-06-9
1. Informática. I. Título
CDD 004

El autor



Gilberto González Rodríguez

Es docente universitario. Actualmente trabaja en la Universidad Politécnica del Valle de México y en el Centro de Estudios Científicos y Tecnológicos del Instituto Politécnico Nacional. Es una persona entusiasta y con ganas de superación personal y profesional. A su corta edad, es maestro en Tecnologías de la información y comunicaciones, y autor del libro Servicio Técnico Notebooks, de esta editorial. Hoy en día, continúa contribuyendo para la editorial como escritor.

Prólogo al contenido

Las redes de cómputo constituyen un elemento predominante en el saber informático, que, sin duda alguna, han proliferado por todo el mundo. Además, día a día, somos cada vez más los que nos unimos para estudiar y diagnosticar las redes. Por tal razón, debemos estar bien preparados y a la vanguardia con respecto a este tema. Mi primer acercamiento real a las redes de cómputo fue al concluir mi primer ciclo de estudiante universitario, cuando una empresa me dio la oportunidad de comenzar a incursionar en algo que, desde hacía tiempo, me gustaba. Fue a partir de ese momento cuando empecé a conocer el apasionante mundo de la realidad mezclada con la afición, y que hoy tengo el gusto de compartir en esta obra. En este libro propongo diferentes soluciones a los problemas que pueden surgir en una red, problemas que deambulan pero que, finalmente, no llegan más allá cuando se ha dado lugar a un conjunto de estrategias de solución. Los invito a formar parte de esta obra, en la que juntos descubriremos cómo enfrentar los inconvenientes más comunes que tienen lugar en las redes informáticas.

Contenido **del libro**











CAPÍTULO 4
MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE UNA RED 61





CAPÍTULO 5
EL CUARTO DE COMUNICACIONES 77



CAPÍTULO 6
SEGURIDAD EN LA RED EMPRESARIAL 89



Capítulo 1

Los problemas más comunes en las redes

Conoceremos los problemas más frecuentes que ocurren en las redes informáticas.



Introducción

Con el paso del tiempo, la mayoría de las **redes informáticas** suelen presentar un sinnúmero de problemas en su infraestructura, tanto física como lógica. Una de las principales causas de los conflictos más comunes se debe al inadecuado cumplimiento de las normas y los procedimientos de seguridad que tienen como fin garantizar un desempeño óptimo del entorno de trabajo.

En la actualidad, existe un amplio menú de soluciones integrales a las cuales podemos recurrir para evitar que un problema alcance niveles difíciles de reparar. Pero, como sabemos, toda solución informática cuenta con un ciclo de vida útil, que desde luego garantiza su funcionamiento por determinado tiempo. Esto depende no solo del técnico, sino también del cumplimiento de los estándares, los modelos y las buenas prácticas establecidas por importantes organizaciones dedicadas a la estandarización (**IEEE**, **ISO**, **ITU** y **ANSI**).

Los problemas que ocurren a menudo en las redes informáticas suelen clasificarse en tres: **problemas en el medio de transmisión** (conectividad física), **problemas de hardware** (dispositivos de red) y **problemas de software** (conectividad lógica). Este contexto incluye a redes tanto **Ethernet** (cableadas) como **wireless** (inalámbricas).

Las redes cableadas y las redes inalámbricas en la actualidad representan el sostén de un sistema infinito de información, a nivel no solo individual sino también corporativo. La demanda por transmitir información de un sitio a otro desde cualquier parte del mundo es un factor que representa una de las razones por las cuales es necesaria la ejecución de planes de mantenimiento que nos

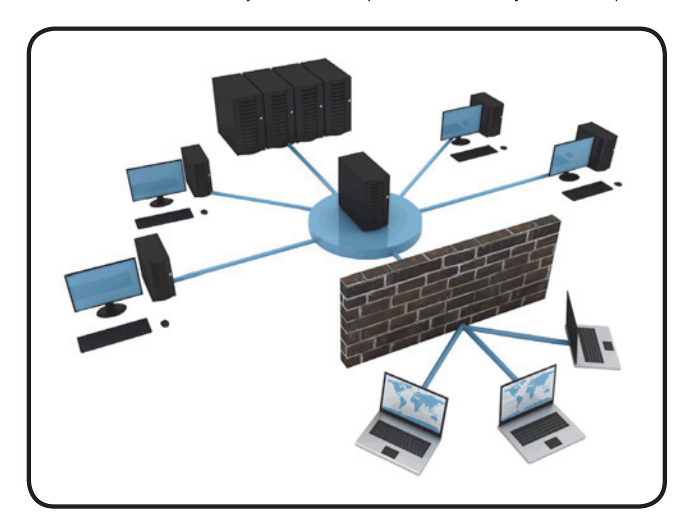


Figura 1. Las redes tienen una vida de diez años; luego, viene el mantenimiento.



Figura 2. **La adecuada configuración de un** router **evita futuros problemas en las redes de datos.**

ayuden a prevenir problemas en el futuro.

La mayoría de los problemas presentes en las redes informáticas provienen de los dispositivos de hardware; sin embargo, no podemos descartar la posibilidad de que pueda tratarse de problemas en la conectividad lógica o en el medio de transmisión.

Se recomienda comenzar a revisar desde la parte física de la que emerge una red (como lo indican los modelos **OSI** y **TCP-IP**) hasta el nivel de aplicaciones para el usuario. Esto nos permite ubicar el momento en que surge el problema, los recursos afectados y, desde luego, la manera de poder solucionar el daño. Es necesario tomar en consideración que en los modelos de capas, estas se encuentran íntimamente relacionadas para mostrar un resultado.

Las redes cableadas y las redes inalámbricas presentan problemas similares, solo que en esquemas distintos. Las redes cableadas suelen ser más complejas en cuanto a estructura física, sobre todo por el tendido del medio de transmisión. Su esquema es más laborioso y requiere de un constante mantenimiento para evitar fallas generadas por el medio ambiente que las rodea. Por su parte,

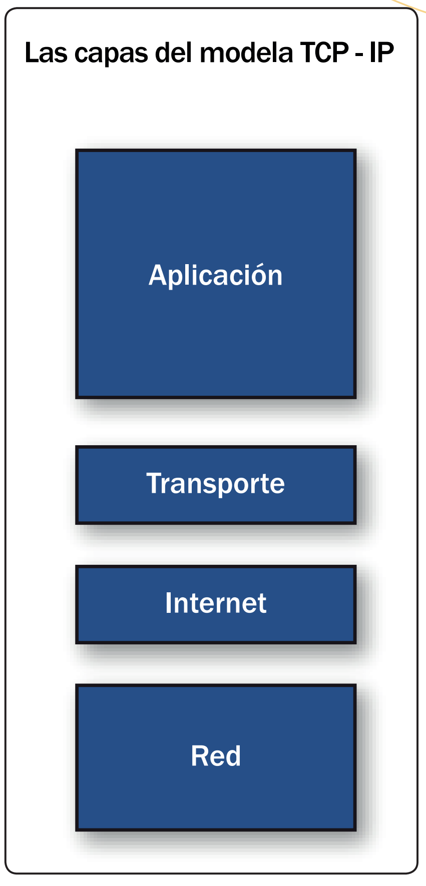


Figura 3. **Los modelos de redes representan un estándar para la industria de las comunicaciones.**

y a modo de ejemplo, las redes inalámbricas simplifican la tarea de tender cables por toda una organización, pues no se requiere más que un conjunto de ondas que se propagan por el aire para emitir señales de comunicación. Más adelante



Figura 4. Las redes convergentes emplean sistemas de seguridad especiales respecto a las redes de oficina.

conoceremos los problemas más frecuentes a los que suelen enfrentarse tanto las redes cableadas como las inalámbricas.

Hoy en día, la tecnología Ethernet y la inalámbrica se conjugan para hacer posible redes de mayor magnitud. Permiten la convergencia, pero sobre todo, la comunicación de una manera más eficiente y siempre al alcance de todo usuario. El conjunto de estas redes da origen a las redes corporativas o empresariales, que también presentan problemas de mediana y gran escala, pues, a diferencia de las redes más pequeñas, en ellas se establecen políticas de seguridad más rigurosas para salvaguardar bancos enteros de información. Las características y los conflictos más comunes en redes corporativas serán descriptos más adelante.

Redes cableadas

Las redes cableadas aún suelen ser las preferidas por muchos usuarios y organizaciones, pero son más complejas de implementar. Cuentan con características que las hacen únicas e irreemplazables, tales como la velocidad, la versatilidad, el soporte y un ciclo de vida aceptable. A menudo, estas redes son las más difíciles de mantener, razón por la cual son más propensas a tener problemas en comparación con las redes sin cable.

Una forma sencilla de clasificar los problemas presentes en una red informática es mediante el análisis de las capas del modelo TCP-IP, el cual se encarga de categorizar las condiciones, los elementos, los protocolos y los dispositivos pertenecientes a la red de datos. Si una red no está bien constituida o presenta alguna falla,



VIDA ÚTIL DEL CABLEADO

Con el fin de evitar problemas de raíz en redes de IT, resulta una buena opción considerar la contratación de un servicio de cableado cuyo ciclo de vida sea superior a los 10 años, con un soporte de dos a tres generaciones de equipo activo.



Figura 5. **Las redes cableadas son propensas a sufrir problemas, debido a su complejidad.**

comenzará a experimentar una serie de inconvenientes que degraden e incluso detengan la comunicación por completo.

En la Tabla 1, describimos los problemas más frecuentes presentados en las redes cableadas dentro de cada capa del modelo TCP-IP.

PROBLEMAS DE LAS REDES CABLEADAS (MODELO TCP-IP)

CAPA	DESCRIPCIÓN DE PROBLEMAS
Capa 1: Interfaz de red	Se producen problemas para establecer redes punto a punto, seguramente derivados de fracturas o de la inadecuada configuración de los medios de transmisión, conexión nula por posibles averías en el adaptador de red (NIC), dificultades de comunicación con diversos nodos del grupo de trabajo (falla en rosetas y paneles de parcheo), problemas electrónicos y sobretensión (voltajes).
Capa 2: Internet	El usuario experimenta problemas relacionados con las direcciones IP, con los dispositivos de red como el módem-router, el switch y los equipos de cómputo (PC, impresoras, copiadoras, servidores, AP, repetidores, etc.).
Capa 3: Transporte	El usuario experimenta problemas de lentitud en el servicio de envío de archivos, el envío de e-mails desde un cliente de correo electrónico, deficiencias de seguridad y protección de datos.
Capa 4: Aplicación	El usuario experimenta problemas de comunicación en la red relacionados con: la recepción de archivos vía FTP, la consulta de páginas de Internet, la recepción de e-mails, las direcciones IP para el acceso a recursos de la red, el acceso a la información deseada, la impresión o reproducción de archivos multimedia (puertos), el monitoreo (en Windows o la ventana de comandos del sistema operativo), etc.

Tabla 1. **Problemas que ocurren en las capas del modelo TCP-IP en las redes cableadas.**

Como podemos observar, los diversos problemas existentes se pueden identificar de una manera más sencilla porque están categorizados por capas. Esto supone que si la red presenta, por ejemplo, problemas de comunicación por una falla física en el puerto RJ-45 del switch, la causa se encuentra en la capa 2 del modelo TCP-IP. Obviamente, si el problema no es el puerto físico sino los cables utilizados, debemos centrarnos en el análisis de los medios de transmisión (capa 1).



Figura 6. **Los errores en la configuración de equipos inalámbricos causan problemas lógicos en la red.**

Redes **inalámbricas**

Para comprender los problemas que a menudo presentan algunas redes inalámbricas, utilizaremos la misma clasificación de las redes cableadas: problemas en el hardware, en el software y en la conectividad (medio de transmisión).

Los problemas en las redes sin cables a menudo se derivan de fallas tanto físicas como lógicas. Por ejemplo, los dispositivos empleados en una red pueden presentar fallas en los puertos de comunicación, lo cual genera un falso contacto que evita la emisión correcta de la señal. Otras veces la falla proviene de una mala configuración en el equipo.

Para la implementación de redes inalámbricas deben analizarse y considerarse muchos factores; algunos de ellos son: el alcance y la frecuencia de la señal emitida, los posibles obstáculos, el equipo físico necesario y, desde luego, la seguridad. Todo elemento que obstruye la



DE LA ASIGNACIÓN A LA RESIGNACIÓN

La asignación de una dirección IP, gateway y DNS es una práctica delicada que necesita de paciencia y conocimiento. Una mala asignación traerá consigo problemas como, por ejemplo, notificaciones de direcciones duplicadas.

libre circulación de una señal en el ámbito de las redes informáticas se llama **obstáculo**. Quizás esta sea la causa principal de los problemas que surgen en las redes inalámbricas. Los ejemplos más representativos son los árboles y las altas edificaciones, cuya estructura es un factor que suele interrumpir la señal propagada.

De estos factores, puede derivarse una serie de problemas que analizaremos más adelante.

Redes **corporativas**

Las redes corporativas se caracterizan fundamentalmente por el uso extensivo de múltiples medios de comunicación. También incorporan un mayor número de tecnologías que las hace las preferidas de cualquier pequeña y mediana empresa. Suelen estar constituidas por un **backbone** o **columna vertebral**, que debe cumplir con un conjunto de estándares para garantizar la funcionalidad total de la red.

El backbone, por lo general, alberga el punto medular de las conexiones física y lógica de la red. En él se concentran los servicios y las conexiones principales (a niveles físico y lógico), por lo que, ante cualquier falla, es recomendable comenzar a hacer una revisión profunda desde este punto. Debemos considerarlo el más importante de la red corporativa.

Cuando el backbone de una organización comienza a presentar problemas, es necesario recurrir a medidas que solucionen el daño, porque de lo contrario se pueden generar pérdidas importantes. En el **Capítulo 6** de este libro describiremos en detalle los problemas frecuentes de las redes corporativas.



Figura 7. El backbone **o** columna vertebral **representa el punto medular en las redes corporativas.**

Problemas a nivel **físico en una red**

Existe una amplia gama de problemas a nivel físico que pueden ocurrir en una red. Estos inconvenientes a menudo se tratan según la tecnología empleada, la topología y la extensión territorial que abarquen. Las redes LAN, por ejemplo, suelen experimentar un menor número de fallas que una red de mayor tamaño (WAN); lo mismo sucede si comparamos una red de oficina central con una corporativa. Sin embargo, siempre debemos estar preparados para evitar ser sorprendidos, pues comenzar a solucionar los problemas desde el principio nos ayudará a comprender un escenario más robusto y complejo.

REDES ETHERNET

Los problemas más comunes a este nivel en las redes Ethernet suelen tener su origen, en primer lugar, en los medios de transmisión, luego en el hardware (como el caso de adaptadores de red, la computadora, impresoras, copiadoras, etc.) y finalmente en la configuración, que puede generar la falta de comunicación de los dispositivos de red. Más adelante veremos este tipo de problemas.

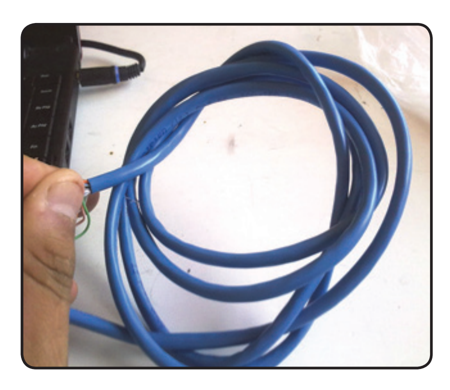


Figura 8. **Un problema típico de las redes a nivel físico está en los medios de transmisión.**

En la Tabla 2 describimos las posibles causas de los problemas que surgen más frecuentemente en los medios de transmisión de datos de una red informática. Para entender la tabla, imaginemos el contexto de una red de 20 computadoras conectadas a un **patch panel** de 24 **puertos RJ-45**, el cual, a su vez, está conectado a un **switch** del mismo número de interfaces. Las computadoras se conectan a un nodo independiente a través de rosetas murales. La red está configurada con un acceso a Internet proporcionado por un router de capa 2. En el Capítulo 2 analizaremos una serie de estrategias para la solución de este tipo de inconvenientes.



ACCESO NO AUTORIZADO

Las violaciones de seguridad en las redes wireless (WLAN) suelen provenir de los puntos de acceso no autorizados, conocidos como **rogue AP**, es decir, aquellos instalados sin el consentimiento del administrador del sistema.

Con respecto a la **Tabla 2**, es importante resaltar que los daños pueden estar presentes de igual modo sobre los puertos físicos en cualquiera de los dispositivos de red señalados (switch, router y NIC). Estos a menudo presentan problemas para la detección de señales portadoras de datos. La principal causa es el constante uso de dichas interfaces, lo que origina que se desolden o se dañen.

PROBLEMAS DEL MEDIO DE TRANSMISIÓN EN UNA RED

PROBLEMA	POSIBLES CAUSAS
El patch cord que va del patch panel al switch de una de las PC no emite luz de ningún color (naranja y verde) desde el panel de puertos del switch.	El patch cord no se encuentra bien configurado o crimpeado. El puerto del patch panel de la PC en cuestión no está bien configurado o crimpeado. El uso constante del cable ha provocado un daño interno o sobre sus conectores.
La adaptadora de una PC solo emite una luz naranja, pero no, de color verde.	La configuración del medio de transmisión no es la adecuada (la adaptadora indica conexión física, pero no, señal de transmisión). El uso constante del cable ha provocado un daño sobre sus conectores. La adaptadora de red está mal colocada o se encuentra dañada.
La red local funciona pero no emite señal de Internet.	El cable que viaja del router al switch está mal configurado, crimpeado o definitivamente dañado. El patch cord que va de la roseta mural a la PC está dañado, mal configurado o crimpeado.

Uno de los puertos del switch no emite ninguna señal.	La configuración del cable del patch panel es inadecuada, o este se encuentra dañado. El patch cord hacia el switch está dañado, mal configurado o crimpeado.
Solo una PC no tiene señal de Internet.	La adaptadora de red puede estar mal colocada o definitivamente dañada. El puerto RJ-45 del patch panel no funciona correctamente. El patch cord de la roseta a la PC está dañado, mal configurado o crimpeado. La roseta mural está dañada, mal configurada o crimpeada.

Tabla 2. **Problemas típicos en medios de transmisión de una red Ethernet.**

OTRAS TECNOLOGÍAS

Existen otras tecnologías de red, como el cableado de **fibra óptica**. Los problemas que surgen en esta tecnología se derivan de una mala conexión por parte del usuario, del maltrato de la fibra y de la distancia a la que es tendida. Los conectores implementados para el crimpeado de la fibra son muy delicados, por lo que es necesario tener cuidado al manipularlos.

REDES INALÁMBRICAS

Como sabemos, las **redes wireless** no usan cables, excepto aquellos que se conectan a un router o equipo de red especializado para las pruebas del dispositivo. Algunos problemas físicos pueden presentarse en los adaptadores de red inalámbricos, los puntos de acceso, los repetidores de señal Wi-Fi e, incluso, en los routers especializados.



PROBADOR DE CABLES

El probador de cable UTP o tester es una herramienta fundamental para el técnico en redes. Permite diagnosticar los medios de transmisión física (configuración y crimpeado), verificar las rosetas y los paneles de parcheo.

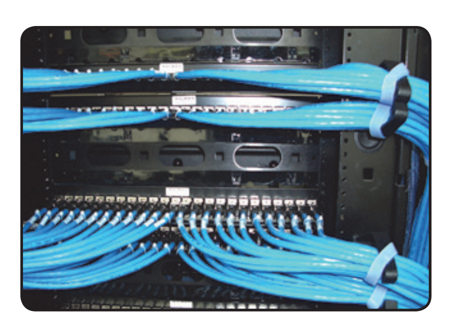


Figura 9. **Una inadecuada configuración de los medios de transmisión provoca un mal funcionamiento de la red.**



Figura 10. **Para evitar problemas en conexiones de** fibra óptica **es necesaria la revisión del medio de transmisión.**

Problemas a nivel **lógico en una red**

Los problemas a nivel lógico también son muy comunes en las redes de datos, sobre todo cuando algún dispositivo de red no está bien configurado. Hoy en día, algunas marcas como **CISCO** o **3COM** han incluido en la mayoría de sus dispositivos de red un sistema operativo que los hace funcionar, el cual es configurado para llevar a cabo la tarea de ruteo de la información.

Cuando un dispositivo de red (Ethernet o wireless), ya sea un router, switch o **Access Point** (este último, para redes inalámbricas), no está funcionando de manera adecuada, seguramente se debe a un problema lógico de configuración. No obstante, podría tratarse



Figura 11. **Una forma de asegurar la emisión de los datos es mediante un dispositivo adaptador adecuado.**



Figura 12. **La adecuada configuración de equipos de capa 2 evita futuros problemas en las redes de datos.**

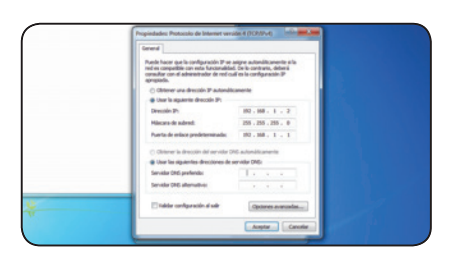


Figura 13. **Las direcciones IP representan el origen de la mayoría de los problemas lógicos en las redes.**

también de un problema físico o en el medio de transmisión. Sin embargo, para poder determinar el origen de la falla, procuremos revisar en primera instancia los elementos físicos, y dejar para último momento la revisión de la parte lógica.

REDES CABLEADAS

La emisión y la recepción de señales de un equipo a otro dependen mucho de la configuración de cada computadora integrada a la red: la configuración adecuada de una **dirección IP**, del **gateway**, los rangos **DHCP** y de los **DNS** utilizados. Estos datos representan la base de la configuración para el resto de los equipos, por lo que es necesario tener pleno conocimiento de ellos para su uso en el futuro.

Otro tipo de problemas lógicos se encuentra en la configuración de los equipos de capa 2, los cuales deben ser administrados.

REDES INALÁMBRICAS

Los problemas lógicos más comunes en las redes inalámbricas son en su mayoría de **cobertura**; por eso es necesario hacer un estudio de la distribución de los equipos en la red, la adecuada configuración de los equipos satelitales, las antenas o **patch**, para evitar inconvenientes de alcance o deterioro de la señal.

Los equipos de red inalámbrica, como routers y AP, deben incluir los parámetros adecuados para garantizar la emisión y la recepción de los datos. Tienen que ser configurados de manera estratégica para salvaguardar la información e impedir los accesos no autorizados.

Derivado de lo anterior, el robo de la señal es un problema común en redes Wi-Fi. Una adecuada administración y protección en la configuración del equipo será suficiente para evitar este tipo de inconvenientes. En el **Capítulo 2** veremos algunas técnicas que sirven para contrarrestar los puntos vulnerables a los que están expuestas las redes inalámbricas.



REDES SEGURAS

Nsauditor es una herramienta que cuenta con un auditor de seguridad destinado a mantener la red de una organización en óptimas condiciones. Cuenta con un instrumento multiuso diseñado para explorar redes ante posibles vulnerabilidades.

Figura 14. **El robo de la señal inalámbrica es uno de los principales problemas de seguridad en las redes.**

Seguridad **informática**

La mayoría de los problemas que se generan en las redes informáticas surge a raíz de la falta de seguridad en la configuración de los equipos. Resulta muy sencilla la colocación de candados que aseguren una computadora, determinada, pero ¿qué podemos hacer para lograr la seguridad de una red?

Actualmente, en el mercado informático existen diversas soluciones de software que permiten el monitoreo de la red. Estas cuentan además



¿CANALETAS DE PISO?

Las canaletas de piso o los canales en forma de media luna son muy comerciales y generalmente empleadas por los técnicos en redes para el tendido del cable Ethernet sobre superficies. Suelen ser de aluminio o plástico rígido.

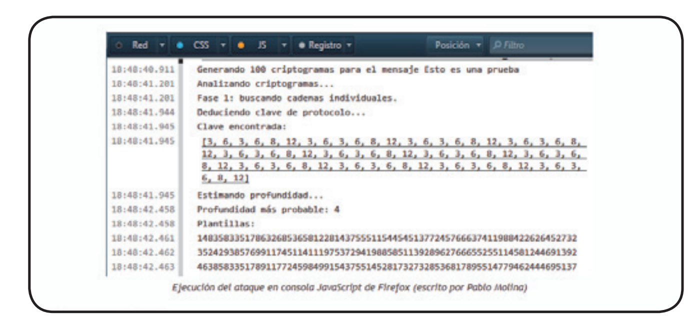


Figura 15. Los métodos de encriptación son una alternativa para mantener protegidos los equipos de una red.

con herramientas que garantizan la seguridad y el control de acceso a la información. Anteriormente, hemos mencionado que uno de los problemas típicos que puede ocurrir, por ejemplo, en cierto tipo de redes es el robo de la señal. Esto se debe a una mala configuración del equipo responsable de brindar la protección informática adecuada.

Desde luego que una alternativa de solución es la colocación de contraseñas seguras o recurrir a métodos de cifrado de datos.

El control de accesos y la detección de intrusos en la red debería representar para todos los usuarios una medida de seguridad eficiente que permita evitar la ocurrencia de problemas.

En el siguiente **Paso a Paso**, vamos a describir un procedimiento muy sencillo que nos permitirá detectar la presencia de intrusos desde cualquier computadora que tenga instalado el sistema operativo Windows y que se encuentre conectada a la red de trabajo.

Antes de comenzar, tenemos que verificar la conexión de todos los nodos con el equipo que actúa como servidor de aplicaciones (la computadora).

Una vez que hemos revisado con cuidado cada una de las conexiones, estaremos en condiciones de comenzar con el proceso de detección. De esta manera, veremos quiénes se encuentran conectados a nuestra red.

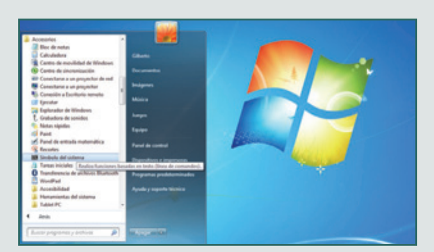


SISTEMA OPERATIVO DEL SERVIDOR DE RED

La adecuada configuración de un sistema operativo para redes evita problemas futuros. Su seguridad garantiza una red estable y sin conflictos lógicos. La mejor opción para Windows son las versiones 2003 y 2008.

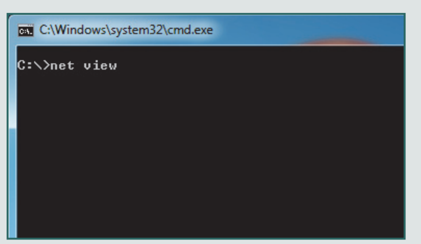
PASO A PASO /1 (cont.)
Detección de intrusos en la red desde Windows





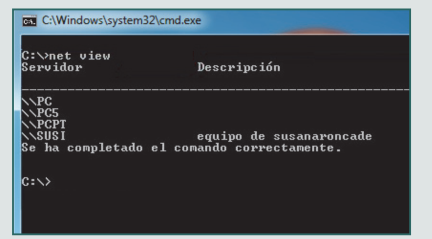
Abra el **símbolo de sistema de Windows** haciendo un clic sobre el botón **Iniciar/Todos los programas/Accesorios/Símbolo de sistema**.

2



Vaya al directorio raíz, escriba el comando **net view** y presione **ENTER**. Espere unos segundos para ver el resultado.

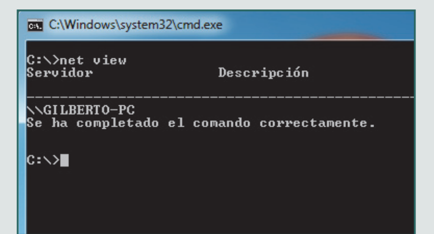
3



En caso de existir intrusos en la red, la pantalla de su terminal mostrará algo similar a esta imagen. Trate de identificar cada equipo que está haciendo uso de la conexión.

PASO A PASO /1 (cont.)





En caso de no existir ningún intruso en la red, la pantalla de la terminal mostrará un mensaje como el de la imagen.



RESUMEN

En este capítulo vimos que pueden ser muchos los problemas que se presentan en las redes informáticas a los que podemos enfrentarnos tarde o temprano. Tener una idea de los inconvenientes más habituales nos preparará para comenzar a buscar soluciones que garanticen un adecuado funcionamiento de la red.

Capítulo 2

Solución de fallas en redes cableadas

Analizaremos las soluciones a los problemas más comunes presentes en las redes de datos.



Problemas físicos **en redes cableadas**

Como sabemos, hoy en día, el cableado estructurado en una empresa debe cumplir con un conjunto de estándares y normativas definidos por importantes empresas de telecomunicaciones para su certificación. Esto se logra haciendo un estudio de la forma en la que circulan los cables sobre cada **rack** situado en el **site** (armario de telecomunicaciones) y de la manera en la que se distribuyen los tubos especiales o canales que alojan los cables (los cuales deben permanecer bien reforzados y sellados). Si alguno de estos elementos no está bien estructurado, habrá consecuencias, y un segmento de la red o la red completa perderá la comunicación.

En el **Capítulo 1** hicimos una clasificación general de los problemas más frecuentes de las redes de datos; describimos algunas fallas críticas y las principales causas que las provocan, con el fin de comenzar a brindar posibles soluciones o contramedidas.

En este capítulo, veremos una serie de estrategias que nos permitirán solucionar los problemas que surjan, que pueden presentarse durante la implementación de la red informática o durante su uso y manipulación.

Antes de comenzar a analizar en detalle las estrategias de solución para los problemas físicos de las redes cableadas, debemos tener en cuenta que existen herramientas destinadas a llevar a cabo dicha tarea. Estas se clasifican de la siguiente manera:

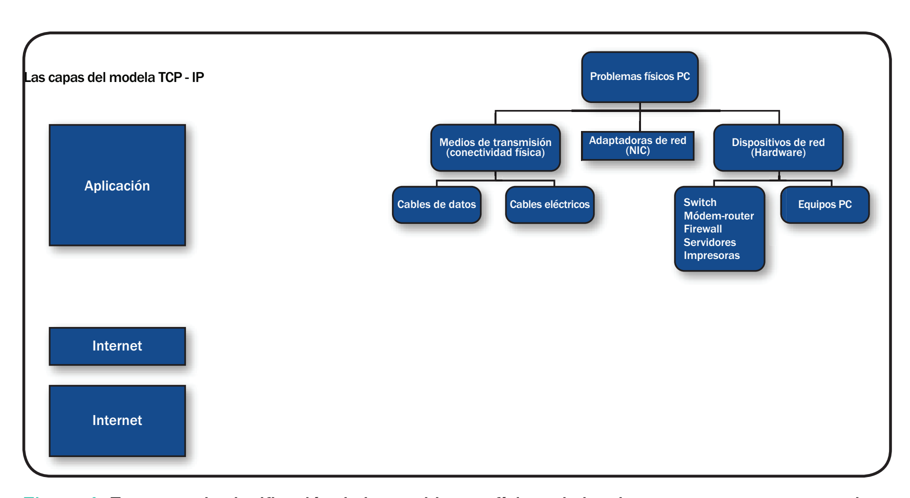


Figura 1. Esquema de clasificación de los problemas físicos de hardware presentes en una red.

- Herramientas para la solución de problemas físicos: son, por lo general, de tipo manual.
- Herramientas para la solución de problemas lógicos: son un conjunto de aplicaciones que tienen como fin auxiliar al técnico para encontrar la mejor estrategia de solución.

HERRAMIENTAS PARA LA SOLUCIÓN DE PROBLEMAS FÍSICOS

Las herramientas más utilizadas para dar solución a problemas físicos en las redes informáticas se encuentran categorizadas en: **herramientas de diagnóstico** y **herramientas manuales** (corrección). En la actualidad, también existen algunas de otro tipo, que serán descriptas en capítulos posteriores.



Figura 2. **Conjunto de herramientas para la resolución de problemas físicos en la red.**

Las que mencionamos a continuación, en la Tabla 1, son muy sencillas de conseguir, porque a menudo están incluidas en la mayoría de los kits para redes, aunque también pueden comprarse por separado y a un precio accesible.

HERRAMIENTAS PARA SOLUCIÓN DE PROBLEMAS FÍSICOS

HERRAMIENTAS DE DIAGNÓSTICO	HERRAMIENTAS MANUALES
Probador de cables multifunción (UTP, fibra, coaxial)	Pinzas para crimpear (múltiple)
Generador de tonos	Herramienta de impacto (Impact tools)
Multímetro	Destornilladores (kit de puntas)
	Pinza universal
	Linterna

Tabla 1. **Clasificación de las herramientas para la atención de problemas físicos.**



Figura 3. La suciedad en conectores de fibra óptica puede corregirse con el uso de un buen kit de limpieza.

Actualmente, también existen kits de mantenimiento preventivo (categorizadas con **herramientas de limpieza**) para retirar la suciedad de los conectores de fibra óptica. En la mayoría de las ocasiones, este factor es la principal causa de problemas en la redes de este tipo.

LOS MEDIOS DE TRANSMISIÓN

Los **medios de transmisión** presentes en la infraestructura de una red cableada pueden ser de dos tipos: de transmisión eléctrica y de transmisión de datos. El primero hace alusión a todo el cableado eléctrico con el que cuenta el área para la colocación de una red informática. Incluye tomas de corriente, apagadores, disyuntor, llaves de corte, reguladores de voltaje, etc. El segundo hace referencia a los cables de datos, como pueden ser: UTP, fibra óptica, coaxial e, incluso, telefónico (generalmente empleado en redes de voz o convergentes).



Figura 4. Con el paso del tiempo, los medios de transmisión de datos pueden ser susceptibles a fallas.



Figura 5. El tester RJ-45 le permite al técnico detectar fallas en un medio de transmisión físico

Transmisión de datos

Los medios de transmisión de datos presentes en una red LAN cableada, a menudo, presentan un conjunto de problemas cuyo origen se encuentra en la forma en que fueron crimpeados. Una inadecuada colocación o configuración de los hilos internos puede impedir que el cable funcione correctamente. Para evitar esta situación, se recomienda tanto el seguimiento explícito de las normas de comunicación (**T568A** y **T568B**), como de la manera en que debe colocarse su conector.

Los conectores o **plugs RJ-45** (para redes Ethernet) son muy delicados: un elemento quebrado o en mal estado ocasionará, sin duda, un mal rendimiento del medio de transmisión.

Cualquiera sea el cable con recubrimiento de plástico que se utilice en la red, puede llegar a presentar rupturas o cortocircuitos internos. La solución más sencilla a este tipo de problemas consiste en retirar el cable completo, lo que implica reemplazarlo por uno nuevo. Antes de sacar el cable, tenemos que verificar su funcionamiento con ayuda del **probador de cables** o **tester**.

Transmisión eléctrica

Los problemas en los medios de transmisión eléctrica suelen ser ocasionados por una



TIERRA FÍSICA

Toda instalación eléctrica debe incluir una descarga a tierra. Si la instalación no se encuentra en óptimas condiciones y con estándares definidos, corremos riesgos de que se produzcan cortocircuitos, incendios y deterioro en las infraestructuras de redes de datos y eléctricas.



Figura 6. **Los medios de transmisión eléctrica pueden alterar el funcionamiento de una red de datos.**

inadecuada inspección del terreno o la colocación deficiente de la descarga a tierra física. Esto puede provocar la avería de todo el equipo de red, porque los reguladores de voltaje pueden resultar alterados al grado de quemarse por descargas eléctricas o variación de voltaje.

Cuando implementamos una red, nunca debemos tratar de hacer convivir un cable de datos con uno de corriente eléctrica, pues podríamos ocasionar un desfase en la señal digital, lo que originaría la pérdida parcial o total de la comunicación. Se recomienda colocar un canal dedicado al medio de transmisión de datos y otro paralelo para el cable de corriente. Desde luego, es bueno consultar el plano del cableado estructurado de la red, porque, según el estándar para la colocación mural de estos dos tipos de medios, se realiza a diferente altura del nivel del piso.

Implementar una red cableada implica el tendido del medio de transmisión (ya sea de datos o eléctrico) por toda el área de trabajo. Muchas veces estos cables viajan por estrechos tubos o canales que los comunican con otro segmento de la red y van a parar al **site** (y de allí, al **backbone**). A menudo, el canal utilizado rodea la habitación; en otras ocasiones, baja de una segunda planta; y en muchas otras, se tiende sobre el piso. Esto demanda la colocación del cable por toda la superficie, lo que origina un maltrato del medio de transmisión por parte de los usuarios y, también, representa un riesgo bastante importante para los involucrados en el uso de la red.

Este problema puede solucionarse colocando el canal adecuado sobre el piso. Este tipo de canal es de aluminio redondeado, conocido como canaleta con forma de **media luna**, y, por lo general, viene seccionado en dos partes: una para la colocación del cable de datos y otra para el cable de corriente que alimenta el equipo de la red.



CABLE TRACKER NETWORK TONE

Es una herramienta manual diseñada para administradores de redes y técnicos del sector. El producto fue creado por la dificultad que existe al intentar rastrear un cable conectado a un circuito activo para una red LAN.



Figura 7. El canal de media luna **evita problemas de maltrato de los cables tendidos obre el piso.**

PANELES DE PARCHEO

Es bien sabido que los paneles de parcheo no son considerados dispositivos, sino elementos pasivos en las redes de datos, cuya finalidad es servir de enlace entre los diferentes equipos de red. Una incorrecta configuración de estos paneles evita la emisión de datos de un **router** o **switch** a cualquier estación de trabajo.

Para evitar problemas de transmisión, es necesario seguir un estándar, una norma, y tener mucha precisión en la banda de configuración del elemento.

LOS ADAPTADORES DE RED

Las tarjetas adaptadoras de red o **NIC** son elementos muy susceptibles a los problemas de comunicación, sobre todo, porque son la principal fuente de enlace entre la computadora y el dispositivo de red. Cuando las tarjetas de este tipo comienzan a tener fallas, lo más recomendable es su reemplazo.

Un síntoma de que la tarjeta de red ya no funciona de manera adecuada es cuando deja de emitir señales luminosas por su superficie. Por lo general, tiene un par de **LEDs** que parpadean cuando se ha reconocido un dispositivo y cuando existe la presencia de datos emitidos, respectivamente.

Otro problema que se deriva del mal funcionamiento de una **NIC** es el deterioro de su puerto de conexión. Cuando dicha interfaz está desprendida del resto de la tarjeta, lo más recomendable es reforzar la soldadura con un cautín de punta y una mínima cantidad de **flux líquido**. Si el puerto presenta suciedad, lo ideal es limpiarlo con la ayuda de aire comprimido.

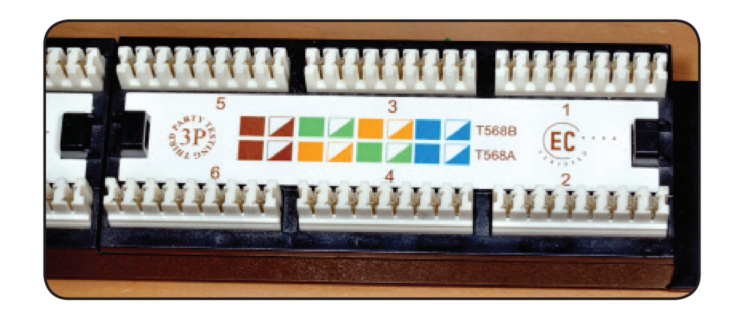


Figura 8. La adecuada configuración de los paneles **de** parcheo **garantiza su buen funcionamiento.**

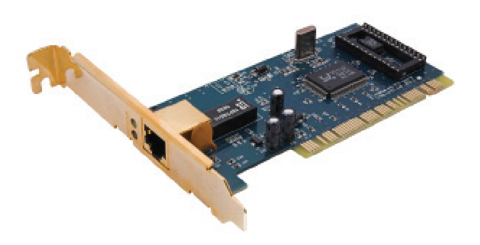


Figura 9. **Una** NIC **es un dispositivo que se conecta a la PC, susceptible a fallas.**

CONEXIÓN FÍSICA DE LOS DISPOSITIVOS DE RED

Todo dispositivo de red cuenta con un conjunto de interfaces o puertos físicos de comunicación sobre sus paneles. Cuando estos comienzan a presentar fallas, lo más probable es que no funcionen los cables. Ante este tipo de casos, debemos intentar cambiar el dispositivo, configurarlo otra vez para activar el puerto o, simplemente, limpiarlo, porque los residuos de polvo suelen generar problemas.

Si se trata de dispositivos de la **capa 2**, puede haber configuraciones inexistentes o interfaces desactivadas. Para revertir el problema, debemos activar el puerto asignando una dirección IP válida o agregar de forma manual un nuevo puerto en sustitución del que presenta fallas.



Figura 10. **Algunas herramientas de limpieza ayudan a mantener en buen estado elementos como una NIC.**

La configuración de equipos como **switches** o **routers** de capa 2 hace posible el funcionamiento físico de sus interfaces (**serial**, **RJ-45**). Para esto, es necesario acceder al sistema operativo del equipo, porque podemos mejorar su funcionamiento mediante una serie de comandos.

EL CUARTO DE COMUNICACIONES

Los problemas más comunes del cuarto de comunicaciones están generalmente derivados de las condiciones ambientales a las que son



CLASE C

En la actualidad, existen distintas clase de extintores, cada uno de ellos utilizado según el tipo de incendio que se desea controlar. Ciertas compañías hacen uso frecuente de extintores de **clase C** en entornos confeccionados para redes de datos y de suministro eléctrico.

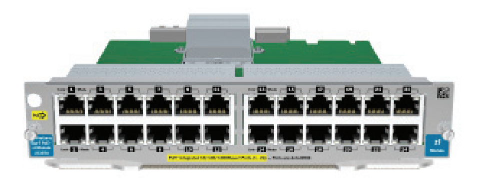


Figura 11. **Los dispositivos de capa 2 permiten la sustitución manual de puertos ante posibles fallas.**

sometidos la mayoría de los equipos que se encuentra ahí. Recordemos que, para evitar problemas en el futuro, es recomendable seguir un conjunto de patrones y medidas de seguridad.

Los cuartos de comunicación son a menudo el prototipo ideal para realizar un análisis de riesgos en materia de seguridad informática, porque la mayoría de los problemas que surgen en este esquema son de tipo físico: incendios, inundaciones, cortocircuitos, etc.



Figura 13. **El extintor es una herramienta útil para contrarrestar incendios en una red.**

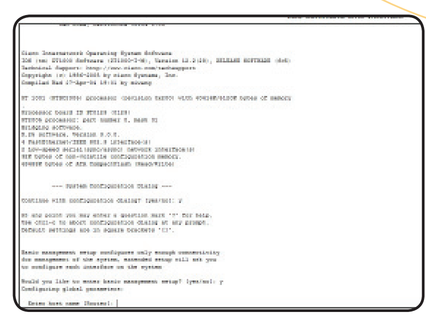


Figura 12. **La configuración del S.O. de un switch hace posible el reconocimiento de sus puertos.**

La manera más simple de evitar este tipo de incidentes es mediante la implementación de medidas de seguridad válidas. Debemos tener siempre un extintor de clase C, especialmente diseñado para usar con cables, que pueden ser los causantes de problemas a raíz del sobrecalentamiento o las condiciones ambientales poco óptimas.

Problemas lógicos en **redes cableadas**

Anteriormente, vimos que la mayoría de los problemas lógicos que surgen en las redes informáticas se debe a la mala configuración de los dispositivos físicos. Sin embargo, esta no es la única causa, porque también suelen presentarse daños derivados de **malware** o código malicioso. No olvidemos que una red de cómputo puede ser muy propensa a virus informáticos si no cuenta con las medidas de seguridad pertinentes.

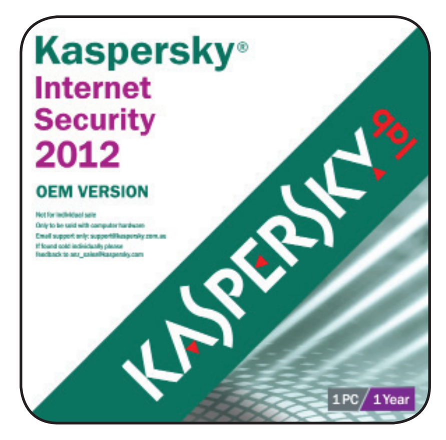


Figura 14. Los antivirus actuales incorporan nuevas herramientas en contra de los ataques a las redes.

Por lo general, los virus se propagan por los medios de transmisión hacia todas las estaciones de trabajo conectadas a la red (computadoras y servidores). Por esto, es necesario tener instalado, desde el servidor, un conjunto de aplicaciones que proteja la integridad de la información. Las políticas de seguridad desde luego juegan también un papel importante para evitar intrusos, accesos indeseados y archivos no autorizados. Estas políticas se asignan, por lo regular, desde el servidor central.



Figura 15. Desde Windows 2008 Server se pueden asignar políticas de seguridad para la red informática.

HERRAMIENTAS PARA LA SOLUCIÓN DE PROBLEMAS DE SEGURIDAD

Siempre debemos estar preparados ante posibles ataques o amenazas que pueden producirse en la red. Para estos casos, recomendamos el uso de algunas herramientas de software que tienen como finalidad mantener a salvo una red completa.

Otra herramienta eficiente para conservar el control de accesos no autorizados o la apertura y cierre de puertos lógicos en la red es el **firewall**, que debe ser configurado para evitar problemas por intrusión.



AXENCE NETTOOLS

Se trata de una herramienta de software que todo administrador de redes debe tener. Es una aplicación fácil de usar, pensada tanto para los profesionales como para los aficionados en el diagnóstico de redes informáticas.



Figura 16. TeamViewer **es una herramienta de control remoto que figura como una opción de monitoreo para redes.**

También existen algunas otras aplicaciones que tienen como fin mantener vigilada la red de datos, además de garantizar su optimización. Se trata de herramientas de monitoreo de nivel software.

En la Tabla 2 presentamos una lista de aplicaciones que a menudo se emplean en redes de computadoras para evitar problemas de inseguridad.

Las herramientas de monitorización a las que hace referencia la tabla son un conjunto de programas que sirven para vigilar el estado de una red. Algunos de ellos son de prueba, aunque son los más utilizados por grandes empresas. Hoy en día, también existen herramientas libres y gratuitas con **licencia GPL**; sin embargo, muchas compañías europeas terminan por implementarlas.

HERRAMIENTAS PARA SOLUCIÓN DE PROBLEMAS DE SEGURIDAD

HERRAMIENTAS DE MONITORIZACIÓN	HERRAMIENTAS DE DIAGNÓSTICO Y CONTRAMEDIDA
NetGong 8.1.	Ethereal
PRTG	Snort
Axence NetTool (kit de herramientas)	GFI LANguard
Nagios (software libre)	Sam Spade
Zaabix (software libre)	ISS Internet Scanner

Tabla 2. Clasificación de las herramientas para la atención de problemas físicos.

Las herramientas de diagnóstico y contramedida son programas cuya finalidad se centra en el análisis de la información, el filtro de amenazas, el rastreo de intrusiones y el escaneo.

CONFIGURACIÓN DE LOS DISPOSITIVOS DE RED

En este apartado, a los fines prácticos, haremos especial referencia a la configuración de equipos CISCO, con el objetivo de ilustrar los puntos clave más vulnerables que tienden a causar conflictos futuros en las redes informáticas.

Los procedimientos que describiremos en el **Paso a paso** son los siguientes:

- Cambiar el nombre de los equipos o dispositivos de enlace detectados en la red.
- Verificar que la configuración de las interfaces del dispositivo estén dadas de alta.
- Asignar de manera correcta tanto las direcciones IP a cada interfaz, como el resto de los parámetros de comunicación.
- Asignar un nombre válido para el grupo de trabajo o dominio en la red.

PASO A PASO /1
Vulnerabilidades en configuración de equipos CISCO

1

```
634880K bytes of ATA CompactFlash (Read/Write)


         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: n


Press RETURN to get started!



Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RED_USERS
RED_USERS(config)#
```

Para cambiar el nombre a un equipo, inicie el dispositivo desde la hyperterminal. Entre en modo privilegiado y acceda a la consola de configuración de la terminal. Ejecute el comando # **hostname**, ingrese el nuevo nombre del dispositivo y pulse **ENTER**. Note que el nombre ha cambiado desde el **prompt**.

2

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RED_USERS
RED_USERS(config)#interface fastethernet0/0
RED_USERS(config-if)#no shutdown

RED_USERS(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

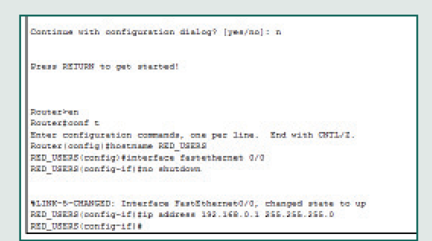
RED_USERS(config-if)#exit
RED_USERS(config)#exit
RED_USERS#
%SYS-5-CONFIG_I: Configured from console by console

RED_USERS#show interfaces
```

Para dar de alta una interfaz o dato relevante, debe emplear el comando # **no shutdown**. Para visualizar el alta de datos basta con teclear el comando # **show** (acompañado del elemento por visualizar) desde la raíz del IOS. Aquí se muestran los elementos que han sido dados de alta.

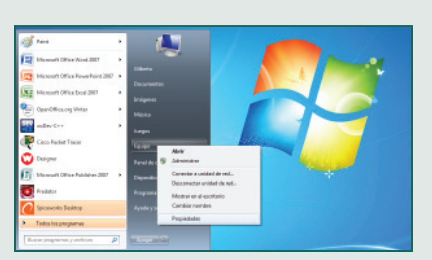
PASO A PASO / 1(cont.)

3



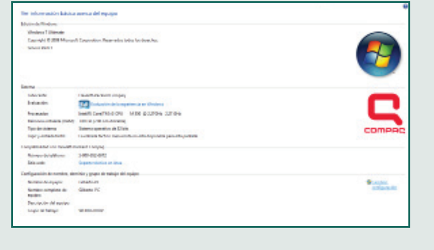
Con el fin de evitar problemas de comunicación de un nodo a otro, configure la dirección IP acompañada de su máscara de red. Ingrese # **`ip address`** más la dirección IP y la máscara de red. Si existe algún error en la configuración, se presentarán errores futuros.

4



Para cambiar el nombre de un grupo de trabajo en Windows, pulse el botón **`Iniciar`**, haga clic derecho sobre **`Equipo`** y, en el menú, seleccione **`Propiedades`**.

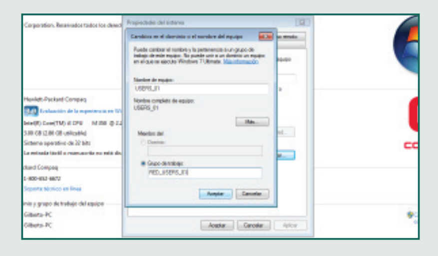
5



Vaya a la parte inferior de la ventana, identifique el campo **`Grupo de trabajo`** y pulse **`Cambiar configuración`**. Una vez dentro de la ventana **`Propiedades del sistema`**, diríjase a la ficha **`Nombre del equipo`** y presione el botón **`Cambiar...`**.

PASO A PASO /1 (cont.)





En **Nombre de equipo** ingrese una nueva denominación. Reemplace también el nombre de **Grupo de trabajo**. Pulse **Aceptar** y reinicie el sistema para validar los cambios efectuados.

Cuando deseamos configurar un router, un módem o un switch, es recomendable cambiar el nombre de dicho equipo para evitar tanto confusiones como duplicidad de dispositivos en la red. Muchas veces conservamos no solo el nombre por defecto que asignan los fabricantes del equipo, sino también las contraseñas. Esto representa un punto vulnerable, que suele ser explotado por ciertos usuarios para robar información (generalmente, en redes inalámbricas).

Las claves más usadas en dispositivos de red son: **admin**, **root**, **toor** o el nombre de la red; por ejemplo: **ermamax**, **56781912**, etc. Para evitar problemas de robo de identidad, hurto de señal e, incluso, de información, se aconseja cambiar tanto el nombre como la contraseña del equipo.

RESUMEN

En este capítulo analizamos diferentes alternativas de solución a los problemas que ocurren en las redes cableadas. Vimos, además, una serie de soluciones integrales (software) para efectuar contramedidas ante posibles amenazas en la seguridad de los equipos de una red de trabajo.

Capítulo 3

Solución de fallas en redes inalámbricas

Analizaremos la solución a los problemas más comunes presentes en las redes sin cables.



El equipo de red **inalámbrico**

Muchos son los posibles errores que suelen aparecer al momento de utilizar una conexión inalámbrica. Estos problemas pueden presentarse tanto en el equipo físico como en su configuración. Para rastrearlos y evaluar la forma de corregirlos, podemos basarnos en el estudio de modelos aplicables a las redes, que sirven como metodología de análisis. Este es el caso del **modelo TCP-IP** y el **modelo OSI** (el primero fue analizado en el **Capítulo 1** de este libro).

También existen algunos enfoques de metodologías que permiten detectar fallas; uno de ellos es la resolución de problemas de arriba hacia abajo. Ante posibles problemas, el enfoque comienza por verificar la configuración de la aplicación y termina con el análisis de interferencia en el radio de enlace. Si se detecta que la señal es baja, se hará la verificación en el radio receptor.

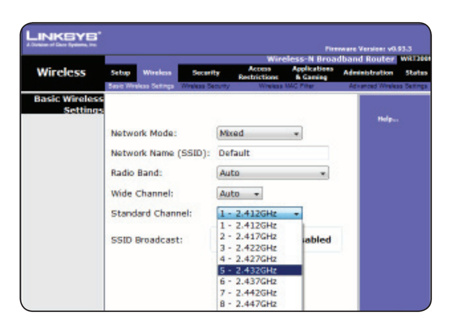


Figura 1. El ajuste del campo `Standard Channel` en el router inalámbrico soluciona problemas por interferencia.

Con el fin de evitar problemas de interferencia, es necesario elegir el número del canal de radio correcto y la frecuencia en el equipo de acceso. Por lo general, el número de canales de frecuencia para un dispositivo de red es de **11** a **14**, aunque su configuración puede variar según el modelo y la marca del equipo. Más adelante, explicaremos los pasos para cambiar este parámetro en nuestra computadora (que se encarga de configurar la interfaz gráfica del router) con el fin de corregir la baja intensidad de la señal inalámbrica o la interferencia en ciertos equipos.

Los dispositivos de red inalámbricos deben estar bien configurados para emitir comunicación en una red. Si por error se omite algún parámetro o dato elemental, sin duda se presentará una serie de inconvenientes importantes.



Figura 2. La adecuada configuración de los AP (access points) inalámbricos es crucial para mantener la comunicación de la red.

El AP no es el único dispositivo físico presente en redes con tecnología Wi-Fi. Otros elementos, como adaptadores, routers inalámbricos y antenas, también deben ser configurados y puestos en marcha para garantizar la comunicación. Esto es necesario al utilizar dispositivos finales o **end devices**, como desktops, notebooks, tabletas wireless, teléfonos analógicos, dispositivos móviles, impresoras y equipos VoIP. Todos ellos son propensos a fallas en caso de no estar dados de alta (identificados con una IP) de manera correcta en la red.

Actualmente, en las redes inalámbricas también pueden presentarse fallas de conectividad, de software y de hardware, o bien una combinación de las tres. En la Tabla 1 se detallan los problemas y soluciones más comunes que experimenta una red Wi-Fi sobre dispositivos finales.



Figura 3. **Ciertos dispositivos, como los teléfonos analógicos, pueden tener problemas de identificación en la red.**

RESOLUCIÓN DE PROBLEMAS EN DISPOSITIVOS FINALES

DESCRIPCIÓN DEL PROBLEMA	ALTERNATIVA DE SOLUCIÓN
La PC no logra conectarse a un sitio web elegido.	Verificar la configuración del firewall (software y hardware) y de los DNS.
La dirección IP de la PC es 169.254.x.x.	Hacer ping hacia la dirección DHCP seleccionada. Verificar que el servidor DHCP esté funcionando adecuadamente.
La PC no se conecta a la red.	Verificar que ningún cable de red esté suelto.
La PC no logra comunicación con otro dispositivo final.	Verificar los permisos del usuario y el estado del dispositivo final.

Tabla 1. **Solución de problemas en dispositivos finales de red.**

PROBLEMAS EN REDES SIN CABLES

Las redes inalámbricas suelen presentar problemas por intensidad de señal, alcance-cobertura, frecuencia, etc. Es habitual que estos vayan acompañados de una **notificación**. En la **Tabla 2** vemos algunos ejemplos.

LOS MEDIOS DE TRANSMISIÓN INALÁMBRICA

Cuando surgen problemas relacionados con la notificación **No hay conexiones disponibles**, suele ocurrir que falla el reconocimiento de algún medio de transmisión o la activación del

PROBLEMAS COMUNES EN REDES INALÁMBRICAS

NOTIFICACIONES	DESCRIPCIÓN/SOLUCIÓN	EQUIPO/ENTORNO AFECTADO
No hay conexiones disponibles	Se puede deber a dos razones: -La conexión inalámbrica no está activa. La solución es activar la conexión manualmente desde el teclado (icono antena Wi-Fi). -No hay una conexión lógica. La solución es dar de alta una conexión lógica.	-Dispositivos finales -Medio de transmisión
Conexión limitada o nula	Ocurre cuando la PC se conecta pero no logra generar la configuración IP; se debe ingresar una dirección de manera manual.	NIC
No se detectan redes inalámbricas	Se debe a que la NIC está deshabilitada. La solución es habilitarla desde el icono Equipo del S.O.	NIC



Conexión detectada pero sin navegación	Error que se muestra cuando la clave de acceso (WEP, WPA) no es correcta o el tipo de encriptación no es compatible entre la NIC y algún dispositivo de red. La solución está en probar con WPA-2 en vez de WEP.	-NIC -Dispositivo de red (router, AP)
Baja señal inalámbrica	Sucede cuando el canal de transmisión asignado en el dispositivo de red no es el adecuado. Se aconseja el manejo de los canales 1, 6 y 11.	Dispositivo de red (router, AP)

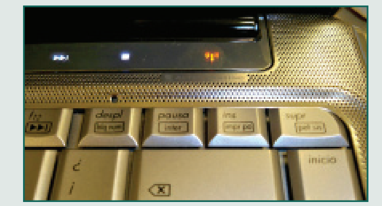
Tabla 2. Descripción de las notificaciones comunes en problemas presentes en redes sin cable.

adaptador inalámbrico desde el dispositivo final (PC). En el siguiente **Paso a Paso** describimos el procedimiento para activar el adaptador de red desde el teclado de la computadora portátil.



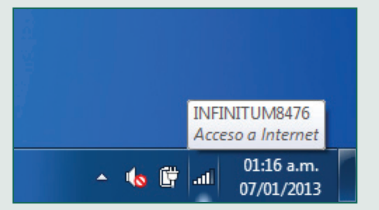
PASO A PASO /1(cont.)





Para activar la tarjeta adaptadora, basta con presionar la tecla o el botón ubicado en el teclado del equipo portátil.





Notará que la apariencia del icono de conexiones inalámbricas ha cambiado. Desde ahora, podrá elegir la red a la que desea conectarse.

El medio de transmisión en una red Wi-Fi es el aire, por donde circulan las ondas de radiofrecuencia. La emisión de dichas señales se logra gracias al manejo de antenas. Por eso, en la actualidad, el diseño de una red inalámbrica requiere contar con un conjunto de elementos apropiados para la transmisión de información.

Para este tipo de redes, a menudo se emplean pequeñas y grandes antenas colocadas de manera estratégica por todo el entorno de trabajo. Estos elementos son portadores de una **banda ancha** (técnica empleada para transmitir y recibir varias señales con diversas frecuencias a través de un medio), que puede ser implementada por varias conexiones, entre ellas, la **conexión por satélite**.

Una conexión por satélite no precisa el uso de ningún cable, porque, en su lugar, emplea una **antena parabólica** para la comunicación bi-direccional. Por lo general, las velocidades de



Figura 4. **Las antenas parabólicas son elementos de transmisión con una carga de 54 kbps.**

descarga son de hasta **500 kbps** ante una carga de entre **54** y **56 kbps**.

Además, se precisa cierto tiempo para que la señal de la antena se transmita al proveedor de servicios de Internet (**ISP**) a través del satélite, que gira alrededor de la Tierra.

El **alcance**, la **cobertura** o radio, la **distancia** y los **obstáculos** son factores importantes que hay que considerar al momento de interactuar con una red inalámbrica. En algún momento, seguramente nos hemos preguntado: ¿qué pasa, por ejemplo, si comenzamos a experimentar problemas por desfase de señal en nuestra red?, ¿o si experimentamos una pérdida de señal parcial o total mientras trabajamos?

Muchos de los grandes problemas para la transmisión adecuada de señales en redes Wi-Fi (no solo en redes pequeñas, sino incluso en las corporativas) se derivan, precisamente, de un mal cálculo o consideración de alguno de los factores antes mencionados.

Para evitar problemas futuros de esta clase, debemos hacer un estudio minucioso sobre la infraestructura de la red mediante el análisis de la **zona de Fresnel**. Comenzamos por calcular el radio de la zona en la que se encuentra la red inalámbrica, y consideramos la distancia entre los objetos hacia el emisor y el receptor, la frecuencia de emisión de la señal (según el canal elegido) y la distancia total entre el emisor y el receptor, en metros.



GUERRA DE COLISIONES

Prácticamente, toda red es propensa a padecer algún problema de funcionamiento. Un problema lógico de gran impacto en las redes es el choque de los paquetes enviados, lo que supone una pérdida total o parcial de la información.

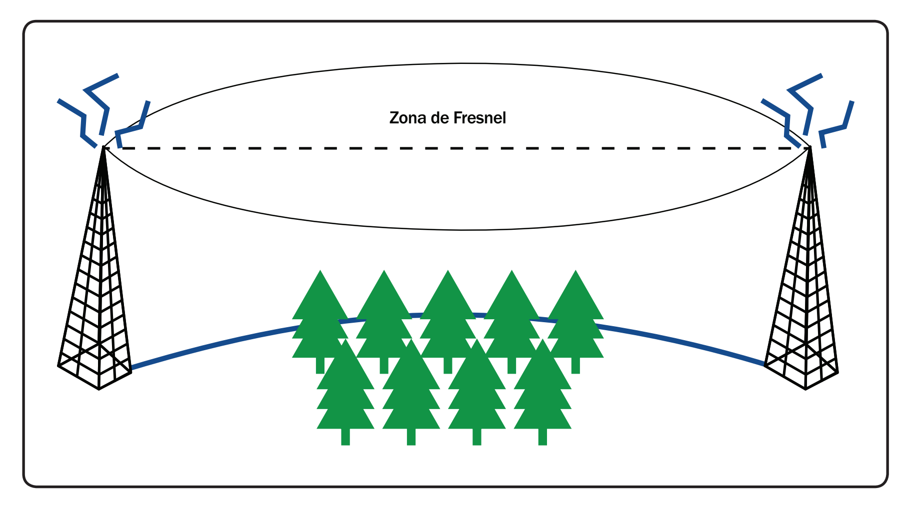


Figura 5. La zona de Fresnel **nos permite hacer el cálculo del radio de una red inalámbrica**.

LOS ADAPTADORES DE RED INALÁMBRICOS

Las **tarjetas de red** (NIC) inalámbricas son a menudo concebidas como un dispositivo de red (incluido prácticamente en todas las computadoras) que permite la emisión de señales en una red de cómputo. Estos adaptadores, por lo general, integran una pequeña antena que hace posible la emisión y recepción de información con la ayuda de un equipo inalámbrico especial. Las **antenas satelitales** o **parabólicas**, a diferencia de las NIC, tienen mayor ganancia, lo que las vuelve ideales para uso corporativo.

Actualmente, existe en el mercado una gran gama de adaptadores especiales para mantener una red inalámbrica funcionando, desde banda ancha móvil (modo USB) hasta pequeños repetidores que cumplen con la tarea de contramedida ante problemas de cobertura de señal.



DISTRIBUCIÓN Y SOLAPAMIENTO DE CANALES

Por lo general, la frecuencia central de un canal se representa en GHz (giga hertz), aunque la frecuencia estándar en el radio de banda de un router inalámbrico oscila entre los 20 y 22 MHz.



Figura 6. Los dispositivos de banda ancha móvil de algunas empresas son un ejemplo de adaptador inalámbrico.

En las redes hogareñas, e incluso a nivel corporativo, es frecuente encontrarnos con notificaciones provenientes de algún dispositivo final, cuyo objetivo es advertirnos de un problema que requiere solución. Un ejemplo de esto es la clásica notificación **Conexión limitada o nula**, que suele aparecer cuando la dirección IP asignada por el servidor DHCP al equipo no es reconocida por la NIC. En el siguiente **Paso a Paso**, explicamos la manera de solucionar este inconveniente, con solo asignar la IP de forma manual.

Antes de comenzar, debemos buscar algunos datos que luego utilizaremos en el paso 5 (dirección IP, máscara de red, gateway y DNS). Vamos a **Inicio/Accesorios/Símbolo del sistema**, ingresamos el comando **>ipconfig** y presionamos **ENTER**. Copiamos los datos que se presentan en pantalla y cerramos la ventana.

PASO A PASO /2
Resolución de problemas: conexión limitada o nula

1

Solucionar problemas
Abrir el Centro de redes y recursos compartidos
07/01/2013

Abra el **Centro de redes y recursos compartidos**, haciendo un clic con el botón derecho del mouse sobre el icono de conexión de redes inalámbricas ubicado en la barra de tareas.

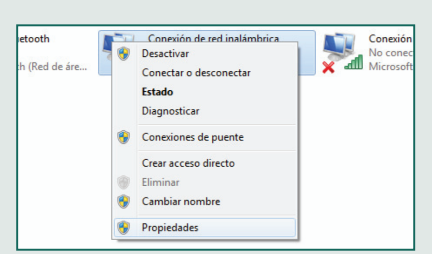
PASO A PASO /2 (cont.)

2



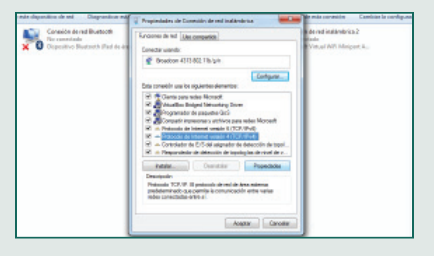
Una vez abierta la ventana, en el panel izquierdo, presione la opción **Cambiar configuración del adaptador**.

3



Haga un clic derecho sobre **Conexión de red inalámbrica** y, en el menú, elija la opción **Propiedades** para desplegar la ventana **Propiedades de conexión inalámbrica**.

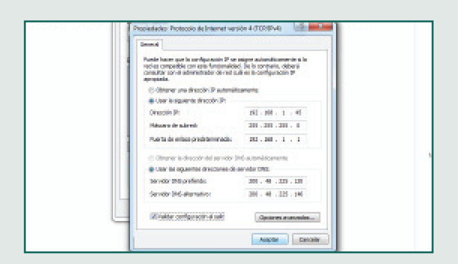
4



Seleccione la opción **Protocolo de Internet versión 4(TCP/IP v4)** y presione el botón **Propiedades**.

PASO A PASO /2 (cont.)



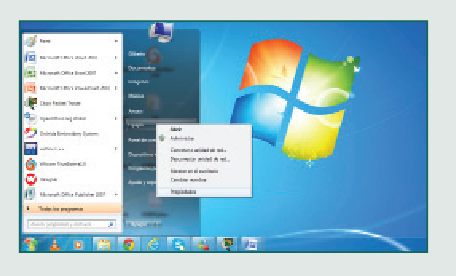


Asigne manualmente los datos que solicita la red para su identificación (el rango de las direcciones asignadas, en general, es proporcionado por el ISP). Para finalizar, pulse el botón **Aceptar**.

Otra problemática similar a la anterior surge cuando no se detectan redes inalámbricas. Esta advertencia aparece cuando la tarjeta en cuestión no está habilitada desde el sistema operativo de la PC. En el siguiente **Paso a Paso** mostramos cómo solucionar este problema:

PASO A PASO /3
Resolución de problemas: no se detectan redes inalámbricas

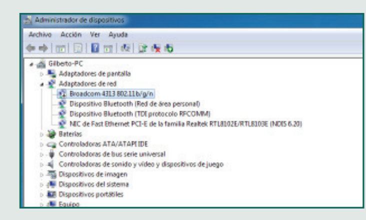




Pulse el botón **Iniciar**, haga clic derecho sobre la opción **Equipo** y, en el menú, seleccione **Propiedades**.

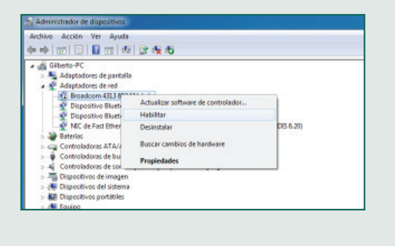
PASO A PASO /3(cont.)





En el panel derecho de la ventana que se abre, pulse **`Administrador de dispositivos`**. En la nueva ventana, despliegue la ficha **`Adaptadores de red`** y ubique la tarjeta que actuará como dispositivo de conexión inalámbrica.





Para activar el adaptador correspondiente, haga clic derecho sobre él y seleccione **`Habilitar`**. A partir de este momento, la NIC ha quedado activa.

Si la computadora sigue sin detectar redes inalámbricas, será necesario evaluar la posibilidad de que haya daños físicos en el equipo, a raíz de los cuales no se reconozca la tarjeta de red. Para descartar dicha posibilidad, lo que debemos hacer es verificar que el nombre de la NIC sea reconocido. Con esta comprobación podremos distinguir cuál es el problema del equipo.



SOLUCIÓN INTEGRAL WI-FI

La combinación de dos tecnologías de red, como PowerLine (redes PLC) y Wi-Fi, permite crear con Dlan 200 AV Wireless N una red informática sin cables y sin las limitaciones que imponen muchos de los obstáculos existentes.



Seguridad en **redes inalámbricas**

La seguridad es un factor fundamental para las redes inalámbricas. Algunos métodos de seguridad que debemos tener en cuenta son:

- Cifrado de datos: para que solo los usuarios autorizados puedan acceder a información a través de la red Wi-Fi.
- Autenticación de usuarios: identifica los equipos que intentan acceder a la red.
- Acceso seguro para invitados.
- Sistemas de control: se encargan de proteger los dispositivos finales y otros equipos de red.

Los equipos inalámbricos, como dispositivos finales, tarjetas adaptadoras, routers y puntos de acceso, por lo general tienen una ficha de seguridad en su interfaz gráfica, que debe ser la misma para cada uno de los dispositivos incluidos en un grupo de trabajo.

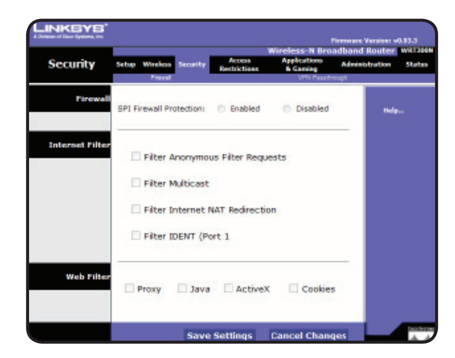


Figura 7. **Ficha** Seguridad **presente en equipos** Linksys **de** CISCO.

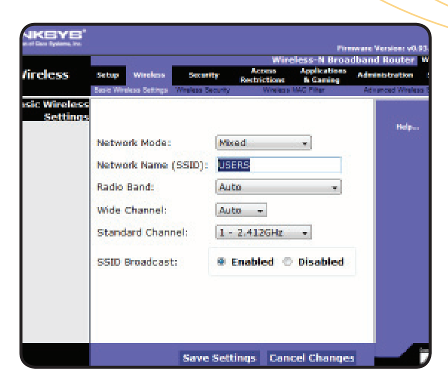


Figura 8. **Cambiar el** SSID **por defecto de un dispositivo de red inalámbrico garantiza mayor seguridad**.

ESTRATEGIAS DE SEGURIDAD

Independientemente de las herramientas de configuración que nos ofrecen la mayoría de los equipos que se encuentran conectados a una red inalámbrica, también contamos con estrategias o buenas prácticas para concretar la tarea de protección del equipo en general. Seguir estas recomendaciones no nos requerirá de trabajo adicional y nos permitirá tener la certeza de que tenemos un entorno más seguro. Algunas de ellas las mencionamos a continuación:

- Cambiar siempre la contraseña por defecto.
- Utilizar una encriptación de tipo WEP o WPA.
- Cambiar las claves WEP con cierta frecuencia.
- Cambiar el SSID por defecto.
- Desactivar el servidor DHCP.
- Activar el filtrado de direcciones MAC.
- Establecer un número máximo de dispositivos que pueden conectarse.
- Desconectar el AP cuando no esté en uso.

Configuración de **los dispositivos de red**

Todos los dispositivos de red que podemos utilizar necesitan una configuración especial para poder emitir señales. A continuación, describimos dos de los principales equipos que permiten el enlace con el resto de los componentes finales: el access point y el router.

ACCESS POINT Y ROUTER

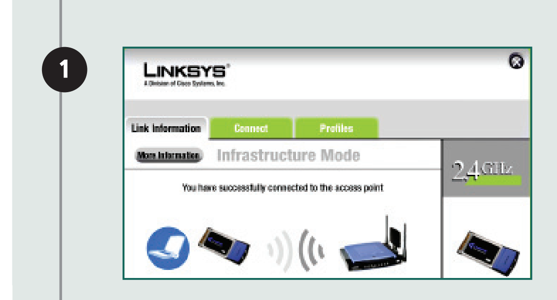
La configuración en los puntos de acceso y los routers es algo crucial para lograr que la red funcione de modo adecuado, es decir, de acuerdo con un estándar y las medidas de seguridad apropiadas. Todo dispositivo de red debe garantizar el envío y la recepción de los datos de una manera segura, por lo que debemos asignar claves de protección o cifrado de la red.

Con esto, evitaremos los problemas futuros o las notificaciones tales como: **Conexiones detectadas pero sin navegación.**

Las claves de acceso o tipo de seguridad más utilizadas son **WEP**, **WPA**, **WPA-2**. En el siguiente **Paso a Paso**, explicaremos el modo de configuración del parámetro de seguridad antes mencionado sobre un access point wireless **Linksys** de CISCO.

PASO A PASO /4
Resolución de problemas: conexión detectada pero sin navegación

1

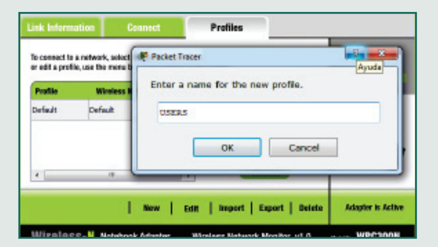


Abra su navegador predeterminado (Mozilla Firefox, Google Chome o Internet Explorer) e ingrese la dirección IP asignada por el ISP. Esto le permite tener acceso a la consola de configuración gráfica del AP.

PASO A PASO /4 (cont.)

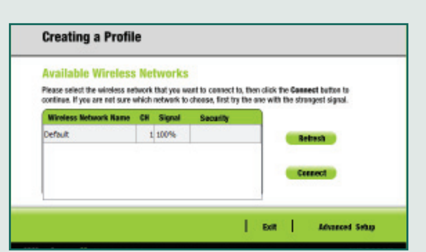


2



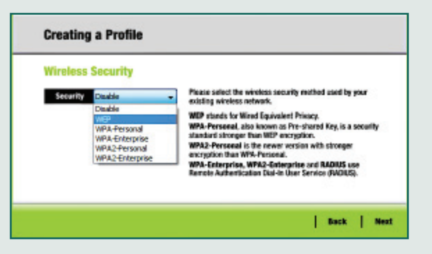
En la ventana **`Autorization`**, que solicita el nombre de usuario y la contraseña, coloque los datos proporcionados por el ISP y presione **`OK`**.

3



Se abrirá la consola de configuración del punto de acceso desde la PC utilizada. Vaya a la ficha **`Profiles`** (perfiles) y presione **`New`** (Nuevo). En la siguiente ventana ingrese el nombre del nuevo perfil.

4

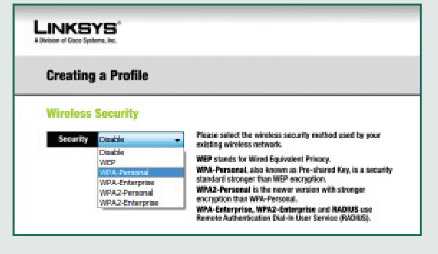


Diríjase a la pestaña **`Wireless`**. A continuación, en la ventana **`Creating a Profile`**, presione **`Advanced Setup`** (configuración avanzada). Ingrese el nombre de la red inalámbrica, los datos de IP, la máscara de red, la puerta de enlace y DNS, y presione **`Next`** (siguiente) hasta llegar a la sección **`Wireless Security`**.

PASO A PASO /4 (cont.)

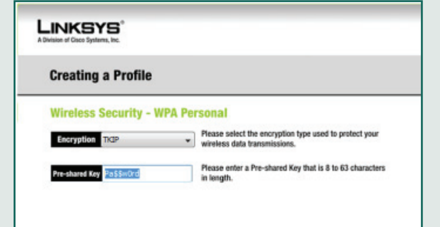


5



En la sección **Wireless Security** (seguridad inalámbrica) tiene que declarar la seguridad de la red. Despliegue el menú **Security** (Seguridad) y elija la clave **WPA personal** (recomendada).

6



Una vez elegido el tipo de protección, ingrese la clave de acuerdo con los criterios que solicita el nivel de autenticación. Finalice el asistente.

Otro problema derivado de algunos dispositivos de red inalámbricos como el router hace que la PC presente notificaciones de **baja señal inalámbrica**. En el siguiente **Paso a Paso**, describiremos el modo de asignación de un canal de frecuencia para evitar conflictos por interferencia o señal baja. Tomaremos como ejemplo un router wireless **Linksys** de CISCO.



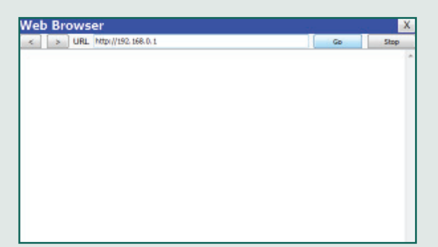
HERRAMIENTA DE CÓDIGO ABIERTO

Nmap es un programa de software de código abierto que sirve para efectuar rastreo de puertos. Se utiliza para evaluar la seguridad de sistemas informáticos y para describir servicios existentes en una red.



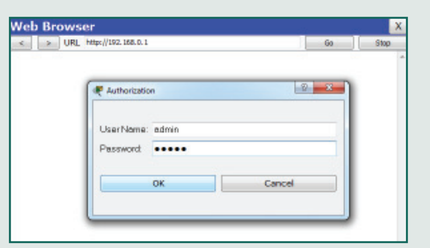
PASO A PASO /5
Resolución de problemas: baja señal inalámbrica





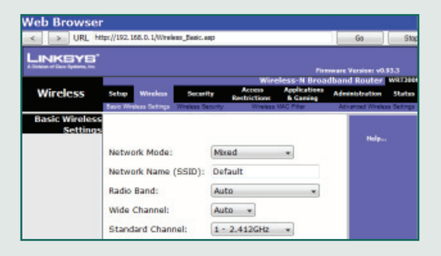
Encienda la PC y el dispositivo de red. Abra el navegador (Mozilla Firefox, Google Chome o Internet Explorer) e ingrese la dirección IP, generalmente asignada por el **ISP**. Esto le permite tener acceso a la consola de configuración gráfica del router.

2



Se abrirá un cuadro que solicita el nombre del usuario y la contraseña. Coloque los datos proporcionados por el ISP y presione **OK**.

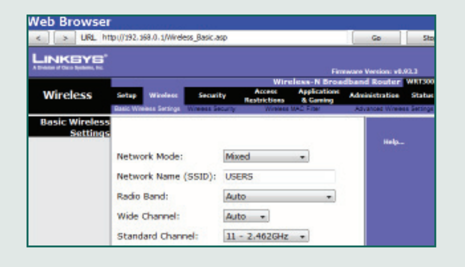
3



Se abrirá la consola de configuración (GUI) del router desde la PC utilizada. Desde la interfaz diríjase a la pestaña **`Wireless`**.

PASO A PASO /5 (cont.)





Vaya al campo **Standard Channel**, despliegue el menú y seleccione algunos de los canales presentes en la configuración. Guarde la información pulsando el botón **Save Settings**. Cierre el asistente de configuración.

ÚLTIMAS RECOMENDACIONES

Ante ciertos problemas presentes en las redes inalámbricas, es necesario tomar una serie de medidas y seguir algunos consejos como los que damos a continuación.

La señal generada por cada punto AP o router tiene un alcance aproximado de 100 metros. Muchos obstáculos (como muros, estructuras metálicas y edificios) suelen afectar negativamente dicho alcance, y la intensidad de la señal inalámbrica se debilita cuanto mayor es la distancia. Para contrarrestar estos inconvenientes, recomendamos distanciar los puntos de acceso y colocarlos en zonas más centrales. Los AP pueden proporcionar una señal de mejor calidad si se ubican sobre techos.

Para obtener mejores resultados, no hay que compartir un único punto de acceso con más de 20 usuarios. Cuanto mayor sea el número de usuarios asociados, más lenta será la conexión. Si la red de nuestra compañía admite un sistema VoIP, se recomienda limitar cada AP a 8 o 10 usuarios, para evitar una posible degradación de la calidad de la voz.

RESUMEN

En este capítulo dimos a conocer alternativas de solución a problemas comunes en redes inalámbricas. Además, explicamos algunos procedimientos para contrarrestar diferentes inconvenientes presentes en la mayoría de los equipos inalámbricos.

Capítulo 4

Mantenimiento preventivo y correctivo de una red

Conoceremos algunas estrategias para realizar el mantenimiento preventivo y correctivo de una red.



El arte **de prevenir**

La prevención es un práctica que todos debemos considerar al momento de estar trabajando tanto en la implementación como en la puesta en marcha de una red informática.

El mantenimiento preventivo es primordial, sobre todo, porque se encarga de garantizar que la red no presente problemas en el futuro (inactividad y fallas en dispositivos). Por esta razón, es aconsejable procurar tener siempre el entorno limpio y en óptimas condiciones. Se recomienda también elaborar planes de mantenimiento periódicos y estrategias válidas de prevención.

En la actualidad, existe un conjunto de técnicas aplicadas en el mantenimiento preventivo de una red que deben emplearse de manera periódica con el fin de evitar problemas. Estas técnicas también están orientadas a salvaguardar la información que vaya a consultarse o manipularse en algún momento dado. Más adelante, en el apartado **Medidas de seguridad en los datos**, conoceremos algunos métodos y daremos consejos para mantener segura la información que se encuentra almacenada en la red de computadoras.

Recordemos que una red de cómputo puede estar compuesta por cientos de máquinas que dependen de un paradigma de interconexión central. Por ejemplo, en el sector corporativo, la red que presente aunque sea un mínimo inconveniente afectará de manera considerable a muchos de los usuarios que interactúen en ella.

A menudo, las redes de computadoras pueden presentar problemas por sobrecalentamiento de sus dispositivos. Esto puede deberse a dos factores ambientales (no intencionales) y enemigos infalibles: el **polvo** y el **calor**. Una alternativa que sirve para evitar daños posteriores es, sin duda, la limpieza frecuente de todo el hardware y los elementos físicos de conexión presentes (switches, routers, PC, tarjetas, impresoras, copiadoras, cables, etc.).

Siempre debemos mantener las salas de red limpias y ventiladas. Para esto, podemos utilizar un aire acondicionado tipo split, procurando cambiar los filtros de aire de manera periódica.

CUIDADO CON LOS CABLES

Siempre que realicemos un mantenimiento, ya sea preventivo o correctivo, será necesario tener especial cuidado con los cables que manipulemos. Debemos empezar revisando el cableado



Figura 1. **Para limpiar los componentes de la redes podemos usar un** blower **o soplador**.



Figura 2. **En salas de cómputo se recomienda mantener el aire acondicionado a una temperatura de entre 22 y 26° C.**



Figura 3. **El uso de** anteojos de seguridad **nos protege ante posibles accidentes en el entorno de trabajo.**

de la red, para asegurarnos de que ningún cable quede fuera de su lugar, porque esto ocasionará una condición insegura importante. El punto clave es etiquetar cada uno de estos medios de transmisión para su identificación posterior.

En el entorno de trabajo, existe una gran probabilidad de peligro al momento de maniobrar los cables para su colocación en la red (de **cobre** o **fibra óptica**). Por lo general, todo el cableado debe tenderse sobre techos y paredes, jamás donde haya algún tipo de obstáculo. Es fundamental usar prendas apropiadas, tales como una bata de laboratorio (lo suficientemente holgada para tal fin) y anteojos de seguridad.

La fibra óptica

Cuando nos encontremos realizando un mantenimiento para prevenir daños en el medio de transmisión, debemos tener presente el uso de anteojos, sobre todo, al momento de manipular cables de fibra óptica (material empleado por muchas empresas). Tomemos en cuenta que para la reparación o preparación de estos elementos a menudo se hace uso de productos químicos que son nocivos para la salud. Aconsejamos leer las instrucciones y atender las indicaciones explícitas que figuran en las planillas **MSDS** (*Material Safety Data Sheet u hoja de datos*) del producto.

Comprometernos con la seguridad ante la maniobra de medios de transmisión como los cables debe ser un hábito para cualquier técnico



USUARIOS PROACTIVOS

En la medida de lo posible, como especialistas en redes, es necesario capacitar a los usuarios de la red de datos mostrándoles cómo conectar y desconectar correctamente los cables. Esto evitará posibles daños causados por impericia.



Figura 4. **Para conocer más sobre planillas** MSDS **podemos consultar** www.osha.gov.

o experto en materia de redes informáticas. Las herramientas utilizadas para la preparación de fibra óptica son, por lo general, elementos punzocortantes, por lo que aconsejamos tener sumo cuidado ante la más mínima manipulación, en especial, al momento en que se dispersen pequeños fragmentos de cristal por el aire, lo que puede provocar severos accidentes.

El uso adecuado del kit de herramientas para la manipulación de fibra óptica evita accidentes. Tengamos siempre cuidado con la vista, pues la luz emitida por este medio conductor puede ser peligrosa. Debemos asegurarnos de tener desconectada la fuente de energía para prevenir que la fibra quede energizada. Siempre tenemos que pararnos sobre alfombrillas oscuras, porque facilitan tanto la detección como la extracción de pequeños filamentos de cristal sobrantes. Asegurémonos de que la superficie sea también antideslizante.

Cable de cobre

Recordemos que el cable de cobre (**UTP**) es un medio que conduce la corriente eléctrica, por lo que la intervención de un rayo o, incluso, la electricidad estática podrían provocar daños en equipos conectados a la red. Para prevenir problemas, recomendamos que, antes de comenzar a manipular este tipo de cables, los sometamos a prueba con la ayuda de un detector de voltaje (**multímetro**).

Los cables Ethernet no son los únicos cables de cobre que vamos a encontrar en el entorno de trabajo donde reside la red. Los cables conductores de voltaje con terminadores de clavija



Figura 5. **Para evitar accidentes, se recomienda la manipulación adecuada de herramientas para fibra óptica.**



Figura 6. **Para evitar problemas de voltaje en cables de cobre, recomendamos el uso de un** multímetro.

(que incluyen todos los dispositivos de red) son susceptibles al deterioro por condiciones inadecuadas del área de trabajo; algunas veces, por sobrecalentamiento; y otras, por emplear niveles de tensión que se encuentran fuera del estándar permitido.

PREVENIR SOBRECARGAS DE VOLTAJE

Las sobrecargas de voltaje suelen producirse comúnmente por rayos (los principales culpables de su variación) o fallas en la planta de luz de un edificio, por lo que es recomendable el uso de equipos reguladores de voltaje, que tienen como fin evitar las descargas eléctricas de manera directa a los equipos con los que trabajamos. Esto garantiza la seguridad tanto del usuario como de los aparatos.

Equipos UPS

Los grandes laboratorios de cómputo que se encuentran en las empresas cuentan con al menos un equipo que se encarga del suministro eléctrico de cada uno de los dispositivos de una red. Estos equipos, que a menudo son utilizados en salas de cómputo, laboratorios, site, etc., reciben el nombre de UPS (*Uninterrumpible Power Supply*). Generalmente son pesados, y ocupan espacios amplios y reservados a ellos. A menudo, conectan gran cantidad de cables de voltaje por toda la sala o construcción donde se estructura la red.

Cabe mencionar que la mayoría de los equipos reguladores destinados a salas de cómputo disponen de un interruptor de activación manual o, simplemente, vienen acompañados de un disyuntor de voltaje que, desde luego, hace posible encender y apagar los equipos que integran nuestra red de trabajo. Esto minimiza la probabilidad de riesgos o accidentes en comparación con el uso de reguladores por cada dispositivo empleado en la red.



¡CUIDADO CON EL CABLE DE RED!

Antes de intentar cortar, pelar o empalmar un cable de fibra óptica, debemos obtener los conocimientos necesarios. Un técnico experimentado debe supervisar dicha tarea hasta garantizar que se han adquirido las habilidades necesarias.



Figura 7. **Los equipos UPS a menudo protegen los equipos de red ante posibles problemas de sobrecarga.**

Como medida de seguridad importante, evitemos ingerir líquidos o transportar alimentos por la zona donde se ubique un UPS, porque resulta peligroso no solo para el usuario, sino también para la red completa.

Ante daños en cables de red (fibra óptica, UTP, voltaje), ya sea por incendio o cortocircuito, recomendamos estar siempre prevenidos y a la orden del día. Para esto, es necesaria la adquisición de extintores de polvo químico. Nunca olvidemos equipar con este elemento la sala de cómputo o red informática. Las redes corporativas están expuestas a una serie de riesgos y amenazas importantes derivados de problemas de sobretensión eléctrica, por lo que es fundamental contar con un extintor de fuegos por cada departamento de la organización. En la Figura 8 presentamos un esquema con las diferentes clases de extintores utilizados en edificaciones.



PAUTAS PARA ELEGIR EL MATAFUEGOS ADECUADO

CLASES DE FUEGOS		TIPOS DE MATAFUEGOS: A AGUA	AB ESPUMA	ABC POLVO ABC	BC DIOXIDO DE CARBONO	ABC HALON
A SOLIDOS	MADERA PAPEL CARTON PASTO TELA TRAPOS	SI MUY EFICIENTE	RE RELATIVAMENTE EFICIENTE	SI MUY EFICIENTE	PE POCO EFICIENTE	SI MUY EFICIENTE
B LIQUIDOS INFLAMABLES	NAFTA ACEITE PINTURAS KEROSENE HIDROCARBUROS y otros líquidos inflamables	NO NO DEBE USARSE	SI MUY EFICIENTE	SI MUY EFICIENTE	SI MUY EFICIENTE	SI MUY EFICIENTE
C ENERGIA ELECTRICA	MOTORES TABLEROS ELECTRICOS TRANSFORMADORES y otros equipos eléctricos	NO NO DEBE USARSE	NO NO DEBE USARSE	E EFICIENTE	SI MUY EFICIENTE	SI MUY EFICIENTE

Figura 8. **Una red de trabajo puede estar sometida a cualquier clase de fuego. Elijamos siempre el extintor adecuado.**

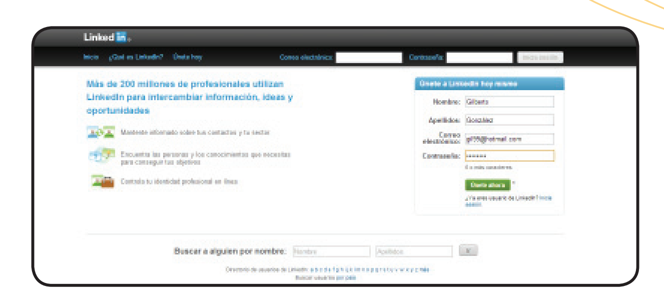


Figura 9. **Para asegurar las sesiones de trabajo en una red debemos usar contraseñas seguras.**

MEDIDAS DE SEGURIDAD EN LOS DATOS

Hoy en día, las redes suelen ser cada vez más vulnerables a muchos ataques informáticos. La información que a diario se almacena puede, incluso, estar expuesta a posibles infecciones, robos, falsificaciones, modificaciones, etc. En redes inseguras, también pueden ocurrir fraudes o sabotajes que provoquen la destrucción total o parcial de las actividades computacionales.

Un método eficaz para proteger sistemas computacionales es emplear herramientas de control de acceso, que cumplen con la tarea de denegar el acceso a usuarios o aplicaciones no autorizadas. Cuando utilicemos este tipo de software, consideremos como medida de seguridad el empleo de contraseñas robustas, las cuales deben de contener por lo menos **8 caracteres**, entre los cuales haya letras del alfabeto (mayúsculas y minúsculas), números enteros y caracteres especiales. Las contraseñas son comúnmente empleadas cuando se desea lograr la conexión a programas informáticos o sistemas operativos.

A continuación, detallamos algunos otros aspectos importantes para la seguridad lógica:

- Hacer respaldos de la información: un **backup** consiste en una copia de los datos escritos en un CD u otro medio de almacenamiento (memoria USB, memoria SD, discos externos E-SATA, etc.).
- Hacer copias de seguridad del disco duro (S.O.) y espejos (arreglos **RAID**): las copias de seguridad permiten preservar la información contenida en una unidad de

CONTRASEÑA PA$$W0RD

La contraseña Pa$$w0rd es, sin duda, la más común en sesiones de autenticación en sistemas Windows para servidores. Quizás esto se deba a que cumple con las especificaciones mínimas de una clave segura.



Figura 10. CloneZilla **es una herramienta de código abierto que hace copias completas de un disco rígido.**

almacenamiento e, incluso, del sistema operativo empleado. Para esta tarea podemos hacer uso de herramientas como **CloneZilla**, **EASEUS**, **Disk Copy** y **XXClone** (Windows). Algunas de estas tienen la facultad de clonar un disco duro completo.

- Proteger los equipos contra accesos no autorizados: podemos proteger todos nuestros archivos con el uso de aplicaciones como **Hide Folders 2012**, que mantienen ocultos los archivos importantes (incluso de sistema) en un lugar seguro. Los archivos quedan protegidos, ocultos, bloqueados o clasificados como de solo lectura.
- Llevar un control de actualizaciones del equipo: una actualización (**update**) consiste en la revisión o reemplazo completo del software que está instalado en cada uno de los equipos de la red.
- Proteger las estaciones de trabajo contra amenazas informáticas o malware: la proliferación de las redes (**LAN**) y el crecimiento de Internet (**WAN**) han abierto muchas vías de infección por virus. Estos programas a menudo son los causantes de daños severos en los equipo de una red. Por tal razón, una medida de seguridad esencial consiste en la adquisición e instalación de un buen antivirus.

PREVENCIÓN DE RIESGOS EN REDES CORPORATIVAS Y CONVERGENTES

Las **redes corporativas** suelen ser el objetivo principal de muchos hackers, crackers, piratas informáticos y personas dedicadas a cometer delitos como sabotaje, hurto y explotación de recursos físicos y lógicos en la red. Este tipo de acciones suele ser más común de lo que imaginamos. Por tal motivo, aconsejamos estar a la vanguardia con respecto a las medidas que permiten mantener segura y protegida la red informática.

A nivel corporativo, la seguridad física es tan importante como la de la información. En la

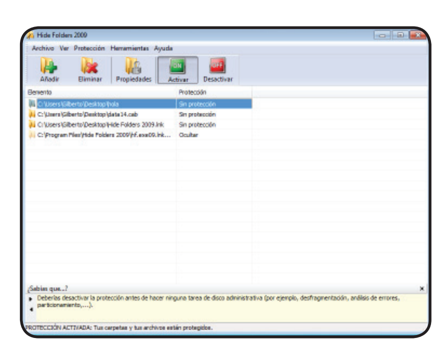


Figura 11. Hide Folders 2012 **es una aplicación que permite ocultar archivos de la PC.**

actualidad, existen diversas formas de proteger la integridad física y lógica de una red. En la Tabla 1 detallamos algunas medidas y alternativas de seguridad.

Cuando hablamos de **redes convergentes**, nos referimos, básicamente, al tipo de red que reúne un número importante de funciones y recursos para la comunicación. Son aquellas

MEDIDAS PARA LA PREVENCIÓN DE RIESGOS

MEDIDA DE PREVENCIÓN	ALTERNATIVAS/DESCRIPCIÓN
Control de acceso a las instalaciones de la red corporativa	-Contratación de personal de seguridad. -Colocación de etiquetas y sensores para controlar la entrada y salida del equipo. -Uso de sensores biométricos que controlan la entrada y salida del personal.
Protección física de los equipos de red	-Adaptación de cables candado flexibles en los equipos de la red. -Colocación de estructuras protectoras en los equipos. -Implementación de tornillos de seguridad en cada equipo de la red.
Protección de los cuartos de comunicaciones	-Mantener bajo llave los sites de comunicaciones (backbone). -Mantener bajo llave los racks de cableado estructurado (usar rack de vitrina).
Rotular los equipos de la red	Identificar equipos mediante tecnología por radiofrecuencia (RFID).

Tabla 1. **Medidas para la prevención de riesgos en redes corporativas.**



Figura 12. **Los cables candado flexibles nos ayudan a prevenir posibles robos de computadoras de la red.**

que hacen posible la integración de recursos como: **telefonía** (tradicional o móvil), **red de datos** (servicio de mensajería instantánea o chat, servicio de correo electrónico), **la radio** y **la televisión** (interfaces multimedia). A menudo, el mantenimiento preventivo de las redes convergentes exige el análisis de las diversas plataformas en las que se concentra la información.

El riesgo más común con el que se enfrentan este tipo de redes en la actualidad es la **incidencia en el rendimiento**, lo que en algún momento puede incluso afectar a los usuarios finales. La contramedida ante este tipo de sucesos es contar con una **solución de monitoreo**, que tenga como objetivo brindar una amplia visión de lo sucedido, identificar las causas que originaron la incidencia y reducir el tiempo de reparación.

Para prevenir problemas en redes convergentes recomendamos controlar, gestionar y monitorear cada uno de los recursos implicados en ella. El **monitoreo** es una medida primordial que permite tener una visión de los problemas que pueden presentarse en la red (a mayor escala en el paradigma lógico en comparación con el físico). La falta de visión impide comprender realmente lo que está sucediendo dentro de dicha infraestructura. Carecer de un servicio como este dificulta también una adecuada gestión de las configuraciones de los dispositivos que integran la red.

Con el propósito de mantener un completo panorama del estado actual y el desempeño de la infraestructura de IT, aconsejamos el uso y la aplicación de **Logicalis**, que consiste en una solución integral para redes que ofrece el servicio de monitoreo de infraestructura.



EL SENSOR RFID

El RFID (Radio Frequency IDentification o identificación por radiofrecuencia) es un sistema de transmisión de datos cuya función es definir la identidad de un objeto (número de serie único) mediante ondas de radio.

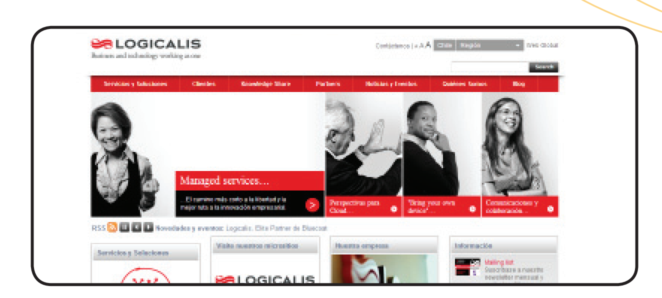


Figura 13. **Podemos obtener información relevante sobre** Logicalis **en** www.la.logicalis.com.

Corrección de **problemas en la red**

El mantenimiento correctivo en las redes informáticas suele ser más frecuente de lo que pensamos. Los problemas que se presentan, por lo general, son a nivel de software. Pero recordemos que el transcurso del tiempo hace posible la aparición de fallas a nivel hardware. Ante esto, recomendamos que, por ningún motivo, dejemos que los problemas menores avancen, pues esto originará inconvenientes más significativos y difíciles de controlar.

Otros de los problemas que surgen se deben al malware proveniente de Internet. Este es el causante de la mayoría de ataques, no solo a la información sino también a los recursos que operan en la red. Más adelante, conoceremos los principales ataques a las redes y la manera de corregirlos.

Recordemos siempre que el técnico en redes debe tener la capacidad de analizar un problema y determinar su causa con el fin de repararlo. Este proceso se denomina **corrección de problemas**.

PRINCIPALES ATAQUES EN LAS REDES INFORMÁTICAS

Como sabemos, Internet es la red más grande del mundo en la cual podemos encontrar una gran cantidad de información y recursos que nos permiten la comunicación. Pero, a la vez, también es un medio peligroso y vulnerable, en el que hay que estar a la defensiva en todo momento.

La gran demanda de Internet ha sido el punto clave para la labor del **cracker** y de un conjunto de usuarios que buscan afectar al resto de los navegantes. A menudo, este tipo de personajes no solo buscan robar información con fines de lucro, sino que incluso han creado una serie de sitios peligrosos en la Web cuyo fin es tanto molestar como infectar de virus a millones de usuarios conectados.

Por lo general, un ataque tiene como objetivo atentar contra algo en particular, de modo que



Figura 14. Kevin Mitnick **es uno de los crackers más famosos de la historia.**

cuando navegamos podemos estar expuestos a muchos peligros, tales como:

- Terrorismo: evitemos proporcionar datos personales que puedan ponernos en riesgo. Este tipo de amenazas afectan en especial a ciertas organizaciones.
- Fraude: algunos sitios recopilan información personal, financiera y bancaria de los usuarios de la red. Estos datos permiten al atacante realizar estafas, vaciado de cuentas y robo de identidad.
- Tortura psicológica: el objetivo principal son los niños, pues a menudo son más propensos a la manipulación y el engaño a distancia. En la red es cada vez más frecuente la existencia de acosadores de menores de edad. Debemos tener cuidado con sitios de contenido pornográfico o violento, que suelen ser usados por estos personajes para torturar al usuario.

Como medida para evitar cualquiera de los ataques anteriores, es recomendable el uso de filtros, políticas de seguridad, antispyware, antispam y la delegación de restricciones de acceso especiales. Esto se puede lograr mediante la configuración individual de cada computadora o desde el servidor de la red.

Estándares **mínimos de seguridad**

Los dispositivos finales de la red informática (que, por lo general, son administrados a



Figura 15. **Las redes sociales son muy propensas a ataques informáticos.**

través de un servidor) necesitan ser configurados de manera independiente con fines de evitar amenazas y riesgos en la infraestructura lógica. Los **sistemas operativos** actuales incluyen una serie de servicios que pueden ayudarnos a prevenir acciones que atentan en contra de la integridad de los datos almacenados en la red. Estos también pueden ser utilizados para corregir problemas que se hayan suscitado en otros equipos.

A continuación, detallamos algunos de los elementos o servicios del sistema operativo que debemos considerar para determinar si una red cumple con los estándares mínimos de seguridad:

- Contar con un **servidor de datos** para almacenar los archivos de la instalación e implementar un proceso de copias bien definido.
- Tener un **dominio** en el servidor para la correcta administración de **permisos** de usuarios y administrar la red de manera fácil.
- Instalar un cortafuegos (físico o por software) para separar la red local de Internet.
- Disponer de un **antivirus actualizado.**
- Todas las estaciones de red deben tener un sistema operativo vigente (Windows 7 o Windows 8) para la correcta validación de los usuarios en el **directorio activo** (dominio).
- Implementar una política de **contraseñas** adecuada (cada usuario de la red debe contar con una contraseña personal).
- Definir una política de **copias de seguridad** efectiva**.**
- Llevar un correcto **mantenimiento** de los dispositivos finales (actualizaciones de software y del sistema operativo).
- Contar con un servicio técnico para la red.
- Poseer las **licencias** de los programas instalados (auditorías).

UNA RED SEGURA Y RESGUARDADA

Un punto bastante descuidado en las redes informáticas es el relacionado con las copias de seguridad de la información. Muchas veces solemos pensar que, con el simple hecho de tener un antivirus instalado en el servidor, ya estamos a salvo de cualquier problema o amenaza. Sin embargo, debemos tener presente que no todos los problemas lógicos provienen de un malware. También existe la posibilidad de que, en un momento dado, los problemas o amenazas surjan de manera no intencional. Los desastres ambientales (derivados de algún fenómeno natural) y la intervención de crackers son ejemplos de esto.



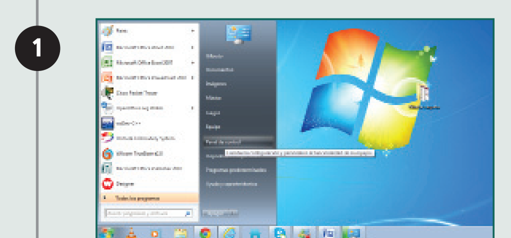
ATAQUES INFORMÁTICOS

Los principales ataques en redes apuntan, por lo general, a los protocolos empleados y a los puertos lógicos de comunicación. A menudo, la suite de protocolos TCP-IP suele ser la causante de la mayoría de los ataques presentes en las redes.

Para estar prevenidos ante posibles desastres, recomendamos la realización de imágenes o copias de seguridad desde el sistema operativo de Windows. En el siguiente **Paso a Paso**, vamos a explicar el procedimiento para llevar a cabo esta tarea.

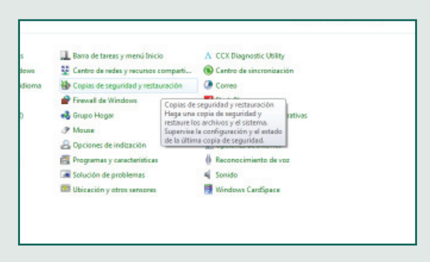
PASO A PASO /1
Generación de la imagen de un S.O. completo

1



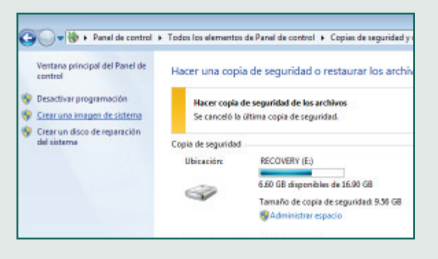
Encienda la computadora y espere a que cargue el Escritorio de Windows. Presione el botón **`Iniciar`** y después vaya al **`Panel de control`**.

2



Desde el **`Panel de control`** seleccione la opción **`Copias de seguridad y restauración`**.

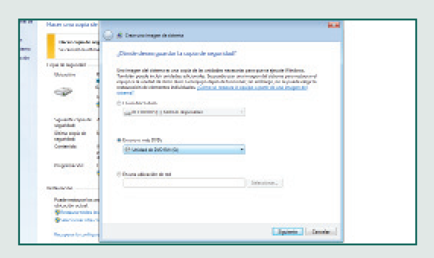
3



Ahora, en el panel izquierdo, seleccione la opción **`Crear una imagen de sistema`**.

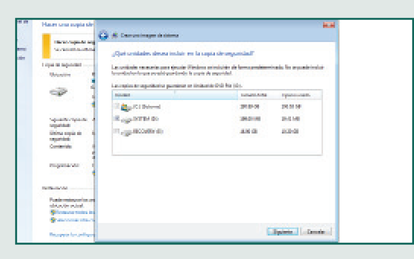
PASO A PASO /1 (cont.)





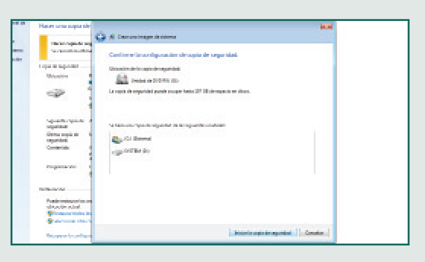
En la ventana que se abre, indique la ubicación donde se almacenará la imagen del sistema. Seleccione **Unidad de DVD RW** y coloque un DVD vacío en la unidad lectora. Presione el botón **Siguiente**.





Elija ahora la unidad que desea incluir en la copia de seguridad. Por ejemplo: **SYSTEM (D:)**. Posteriormente, presione el botón **Siguiente**.

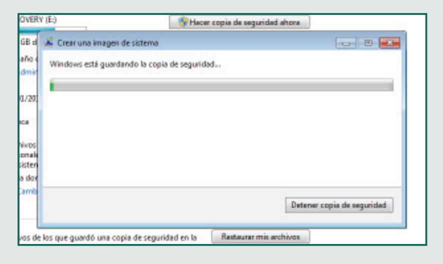




Verifique que los datos de su elección sean los correctos. Si está seguro de la información proporcionada, presione el botón **Iniciar la copia de seguridad**.

PASO A PASO /1 (cont.)

7



Desde este momento, no interrumpa por ningún motivo la copia de seguridad. Espere hasta que finalice. Cuando esto suceda, la imagen quedará creada en el volumen asignado.

La imagen del sistema generada con anterioridad puede utilizarse posteriormente con fines de copia para la configuración de los equipos restantes de la red, lo que hace posible que se recorten los costos en tiempo y se simplifiquen las tareas de configuración de los parámetros de seguridad desde el sistema operativo.

RESUMEN

En este capítulo dimos a conocer algunos consejos para prevenir futuros problemas en las redes de cómputo. Hicimos un breve recorrido por las redes locales, hasta las redes corporativas y convergentes. En próximos capítulos conoceremos las condiciones del área de trabajo de una red.

Capítulo 5

El cuarto de comunicaciones

Conoceremos las condiciones de seguridad que debemos tener en el cuarto de telecomunicaciones de una red.



El área de trabajo **y el cuarto de telecomunicaciones**

Las redes informáticas de las empresas, por lo general, se dividen en dos espacios físicos por cada planta o piso: **el área de trabajo** y **el cuarto de telecomunicaciones**. En las redes más pequeñas no siempre se implementa este tipo de infraestructura, porque carece de sentido si la red está limitada en espacio y envergadura.

El área de trabajo de una red es un espacio totalmente distinto del cuarto de telecomunicaciones. Algunos ejemplos del primer entorno pueden ser un departamento organizacional (ventas, compras, sistemas), una oficina central (sala de juntas, área de capacitación) y un laboratorio. Allí se albergan todos los recursos indispensables para satisfacer las necesidades del usuario final, que pueden ser informáticos (computadoras, copiadoras, impresoras, etc.) o de acondicionamiento (extintores, aire acondicionado, disyuntores, UPS, etc.). Debe cumplir con una serie de características estándar, que garanticen un área libre de riesgos y condiciones inseguras.

El cuarto de telecomunicaciones es un espacio más reducido que el área de trabajo de una red (sus dimensiones varían de acuerdo con la organización), que debe permanecer aislado del entorno donde se ubican los usuarios finales. Su implementación en las empresas tiene la finalidad de albergar tanto el cableado estructurado de la red, como ciertos dispositivos y elementos: concentradores, conmutadores, firewall, servidores dedicados (correo, impresión, antivirus, vigilancia), monitores, paneles, armarios, soportes, etc. Los cables deben ubicarse en armarios para evitar cualquier contacto con manos inexpertas. La seguridad del equipo que se encarga de hacer funcionar un área de trabajo o red organizacional es un aspecto que debe tomarse muy en serio.



Figura 1. **El** área de trabajo **de una organización concentra los equipos destinados a los usuarios finales.**



Figura 2. **Por seguridad, los equipos y el cableado son resguardados en armarios dentro del cuarto de telecomunicaciones.**

Por seguridad, cualquiera de estos equipos tiene que permanecer bajo llave y debidamente resguardado. El administrador de la red será la única persona que tenga acceso a este lugar, porque se ocupa de revisar, diagnosticar y corregir los problemas que puedan ocurrir.

CONDICIONES DE SEGURIDAD

En el **Capítulo 4** detallamos algunos elementos de seguridad que son indispensables en el área de trabajo de una red. En esta sección, vamos a focalizarnos en el equipamiento del cuarto de telecomunicaciones.

Además del extintor de incendios, el aire acondicionado y los UPS, existen otros elementos que debe contener un área de trabajo donde se ubica una red informática.

Soportes para cables

Los **rieles en forma de escalera** forman una guía segura por donde viaja el medio de transmisión utilizado. Su recorrido comienza en el entorno de trabajo y termina en el cuarto de telecomunicaciones. Algunas empresas simplemente hacen uso de canaletas o ductos para aislar el cable utilizado. De esta manera, evitaremos problemas de funcionamiento o accidentes.

Si preferimos colocar los cables sobre el suelo o el techo, debemos utilizar **piso** o **cielo falso**. Para el área de trabajo siempre tenemos que hacer la instalación de cables por paredes o cielo. En cambio, para el cuarto de comunicaciones la instalación debe realizarse sobre paredes y piso; es importante evitar las instalaciones sobre techo falso. Esto deriva del tendido de la canaleta, que por norma está colocada a una distancia más próxima del nivel del piso que del techo.



IDENTIFICACIÓN DE NODOS

Un nodo representa el puerto donde se conecta un equipo en la red. Recomendamos la identificación de nodos en ambos extremos del cable (del rack al dispositivo final). Las cajas de cada nodo son también identificadas, para facilitar la ubicación de fallas.



Figura 3. Los rieles en forma de escalera permiten el transporte seguro del cableado de la red.

Este escenario facilita la adecuada distribución de los cables al rack, y evita el uso de mayor cantidad de cable.

En las áreas de trabajo, suelen colocarse racks de vitrina empotrados sobre las paredes a unos cuantos centímetros del techo. Aquí el escenario cambia, pues resulta más sencilla una adaptación desde arriba.

El número y el tamaño de los ductos utilizados para acceder al cuarto de telecomunicaciones varían con respecto a la cantidad de áreas de trabajo que llegan a él. Sin embargo, se recomienda tener por lo menos tres ductos de 4 pulgadas para la distribución del cable del **backbone**, tal y como lo establecen algunas normas y organizaciones, como **ANSI/TIA/EIA-569**. Además, los ductos de entrada deben contar con elementos de retardo de propagación de incendio.

Extintor de incendios

Otro elemento importante que es necesario tener en el cuarto de telecomunicaciones,

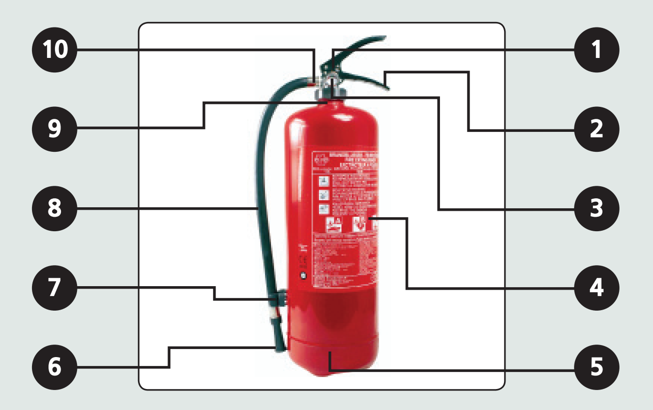


CCNA PRESENTE EN LAS REDES

Las currículas CCNA de CISCO incluyen, entre otros recursos, una serie de prácticas de laboratorio sobre resolución de problemas de redes empresariales. Para más información, podemos acceder a: **www.cisco.com/web/learning/netacad/index.html**.

además del que se encuentra en el área de trabajo, es el extintor de incendio. En el **Capítulo 4** explicamos la clase de extintor que precisamos; en este apartado describiremos las partes que lo conforman mediante una **Guía Visual**. El reconocimiento de sus componentes nos ayudará a comprender la manera correcta de utilizarlo.

GUÍA VISUAL /1
Partes de un extintor de incendio



1. Pasador de acero inoxidable: es una palanca de seguridad que comúnmente viene acompañada de una correa plástica. Evita descargas accidentales y alteraciones del extintor.
2. Manijas de acero inoxidable: permite el transporte y uso del extintor. Cuenta con un diseño ergonómico que permite una mayor comodidad durante su manipulación.
3. Manómetro con protector plástico: es una válvula de fácil lectura, que se encuentra protegida para soporte de impactos.
4. Placa de producto: es una placa de identidad, que incluye las instrucciones de uso, el tipo de extintor y los componentes químicos.

GUÍA VISUAL /1 (cont.)

5. **Cilindro**: fabricado con tapas troqueladas y soldadura por resistencia eléctrica. Soporta impactos y vibración.
6. **Boquilla plástica**: el tamaño depende de la clase de extintor. Las boquillas de amplia salida permiten una mejor descarga y el buen barrido de la base del fuego.
7. **Soporte de manguera**: algunos modelos incorporan un simple sujetador o cinturón de acero que rodea al cilindro; se encarga de mantener la manguera sujeta en su sitio.
8. **Manguera de caucho**: fabricada con acoples y ferrules en aluminio. Soporta la presión de trabajo y permite una operación segura.
9. **Tubo sifón**: se encuentra en el interior del cilindro; generalmente está fabricado en material resistente que garantiza un buen funcionamiento.
10. **Cuerpo de válvula y vástago**: sujeta la manguera. Es de aluminio, y el vástago, de acero inoxidable, lo que garantiza mayor durabilidad.

El material con el que están construidos los extintores depende del fabricante, aunque la mayoría sigue un estándar que garantiza su duración y resistencia. El cuarto de telecomunicaciones también debe ser equipado con un extintor de clase C.

Puerta de acceso

Otra condición de seguridad con la que debe contar el área de trabajo está relacionada con la salida principal. La puerta tiene que ser, preferentemente, metálica, y contar con un mecanismo de apertura hacia afuera al ras del piso. Por ningún motivo puede tener postes centrales.

Piso antiestático

El polvo y la electricidad estática son elementos del ambiente que deben ser disipados de manera constante. Una forma de evitarlos es



EL TECHO Y EL PISO FALSOS

Los techos falsos están compuestos por material frágil y se los conoce con el nombre de **plafones**. En cambio, los pisos falsos son más resistentes y muy usados en la adaptación de cuartos de telecomunicaciones.



Figura 4. Las cerraduras de doble paso son ideales para puertas en áreas de trabajo.

mediante el uso de piso de cemento, cerámica, loza o similar, tanto en el área de trabajo como en el cuarto de telecomunicaciones. Por ningún motivo podemos admitir el uso de alfombras, porque este elemento puede traer severas consecuencias, tales como: daños internos a los equipos conectados por descarga electrostática (ESD), y avería en cables (ubicados en el rack) y en los puertos físicos de conexión.



Figura 5. **Los eliminadores de electricidad estática son una buena opción para el cuarto de telecomunicaciones.**

Refrigeración del ambiente

La **refrigeración ambiental** del cuarto de telecomunicaciones es distinta de la empleada en el área de trabajo. Para habitaciones que no cuentan con equipos electrónicos debe considerarse una temperatura de entre 10 y 35 grados centígrados, mientras que la humedad debe mantenerse en escalas del 85%. Además, se recomienda un cambio de aire por cada hora.

Para cuartos que poseen dispositivos electrónicos, la temperatura debe estar calibrada en una escala de entre 18 y 26 grados centígrados, y la humedad relativa debe mantenerse entre 30% y 55%.



Figura 6. **El aire acondicionado siempre debe instalarse cerca del techo.**



Figura 7. **Las rociadoras de agua pueden contrarrestar los problemas de incendio.**

Drenaje del piso

El cuarto de telecomunicaciones tiene que estar libre de cualquier amenaza de inundación, por eso es importante verificar que no haya ninguna tubería de agua sobre él o en sus alrededores. En caso de requerir el uso de agua, se debe contar con un dispositivo de **drenaje de piso**. En algunas ocasiones, los extintores no son suficientes, por lo que se recurre al uso de regaderas contra incendio. En estos casos, recomendamos la instalación de canales para drenar el goteo de las rociadoras.

Iluminación

El cuarto de telecomunicaciones jamás debe estar oscuro, porque esto generaría condiciones inseguras; es por eso que recomendamos una buena iluminación. Esta debe estar a un mínimo de **2,6 m** del piso, mientras que para áreas de trabajo puede estar, incluso, a una altura mayor. Además, se aconseja pintar las paredes de un color claro para mejorar la iluminación. No debemos olvidar las luces de emergencia, para estar preparados ante posibles fallas eléctricas o cortes de luz.

INSTALACIÓN ELÉCTRICA

Tanto el cuarto de telecomunicaciones como las áreas de trabajo deben contar con la cantidad de tomacorrientes suficientes capaces de alimentar los dispositivos almacenados en los anaqueles (racks) de la habitación.

Por esta razón, recomendamos tener como mínimo dos **tomacorrientes trifásicos dobles** de **110-120 V** de corriente alterna. Su instalación evita el uso de enchufes adaptadores trifásicos adicionales, que pueden afectar la

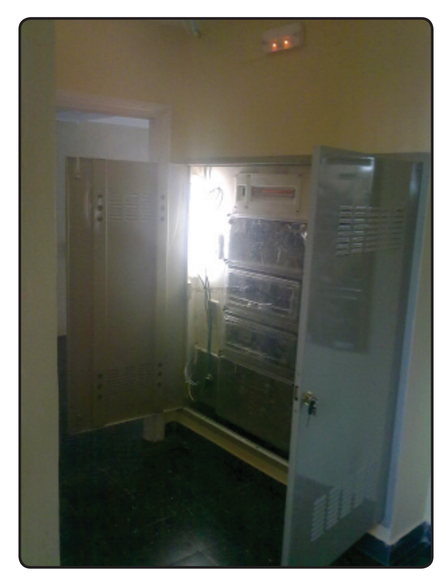


Figura 8. **Las lámparas de emergencias contrarrestan problemas de iluminación en el cuarto de telecomunicaciones.**

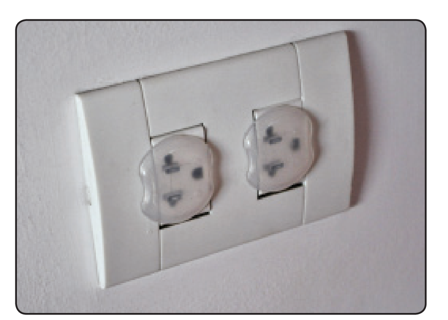


Figura 9. **Los protectores de tomacorrientes evitan problemas de funcionamiento por suciedad.**



Figura 10. **Las centrales telefónicas hacen posible el uso de voz sobre Internet (VoIP).**

polaridad de los equipos conectados. Estos deben rodear la habitación y estar distribuidos a una distancia de 1,8 m el uno del otro, y a 15 cm del nivel del piso.

También debemos tener un equipo de alimentación eléctrica de emergencia con activación automática ante cortes de energía.

Por último, para evitar los problemas por descargas que pueden afectar a los equipos, incluso a los UPS, aconsejamos la implementación de descargas a tierra con conexión de 6 AWG, con especificaciones asignadas por las normas ANSI/TIA/EIA-607.

La instalación **VoIP**

Llevar a cabo la instalación de recursos VoIP sobre una red de cómputo no es algo complejo, pero requiere paciencia, conocimientos básicos y mucha destreza.

La incorporación de estos recursos es cada vez más común en las organizaciones. Por ejemplo, algunas pequeñas y medianas empresas emplean esta tecnología para realizar llamadas y mantener la comunicación con otros sectores o sucursales.



ESTÁNDARES Y NORMAS IT

En el ámbito de las redes, es común encontrar un conjunto de estándares y normas de comunicación. Uno de ellos es el estándar ANSI/TIA/EIA-568-A de alambrado de telecomunicaciones para edificios comerciales.

Para comprender la esencia de la tecnología VoIP y su relación con el cableado estructurado, vamos a describir un conjunto de componentes de esta tecnología.

El primer elemento que debemos conocer es la **centralita telefónica** (**PBX**, *Private Branch Exchange*; y **PABX**, *Private Automatic Branch Exchange)*, que consiste en un equipo privado que hace posible gestionar llamadas telefónicas internas en una empresa. Además, da la posibilidad de compartir las líneas de acceso a la red pública entre varios usuarios, quienes se encargan de enviar y recibir llamadas desde cualquier lugar permitido.

Otro elemento es la **línea telefónica** para la conexión a Internet (banda ancha), que puede estar conectada a un concentrador independiente y, desde allí, a la centralita. Una central telefónica tiene un lugar reservado en el cuarto de telecomunicaciones.

Las centralitas telefónicas, al igual que cualquier otro dispositivo de la red, también son propensas a sufrir problemas. El más común es la distorsión de audio. Hoy en día, existen varios factores que pueden afectar significativamente la calidad de audio de las llamadas. Para solucionar este inconveniente, podemos probar los siguientes procedimientos:



Figura 11. La UC 500 es una centralita para pymes de CISCO que soporta de 8 a 104 usuarios.

- **Reiniciar dispositivos**: recomendamos reiniciar tanto la computadora como la centralita, porque de esta forma se renueva la conexión.
- **Elegir servidor**: podemos hacer ping a cada uno de los servidores, para comprobar las latencias y elegir la mejor opción.
- **Prueba con softphone**: para eliminar la posibilidad de que la computadora o la centralita sean las causas del problema, podemos recurrir a las aplicaciones softphone. Estas soluciones se usan para realizar o recibir llamadas. Zoiper Classic o X-Lite son las recomendadas por el soporte técnico de VoIP.



TOMACORRIENTES UNIVERSALES

Actualmente, existe un conjunto de soluciones para la industria eléctrica y las telecomunicaciones. Los tomacorrientes universales son una opción ideal para conectar cualquier tipo de medio certificado. Su uso es muy común en redes informáticas y eléctricas.

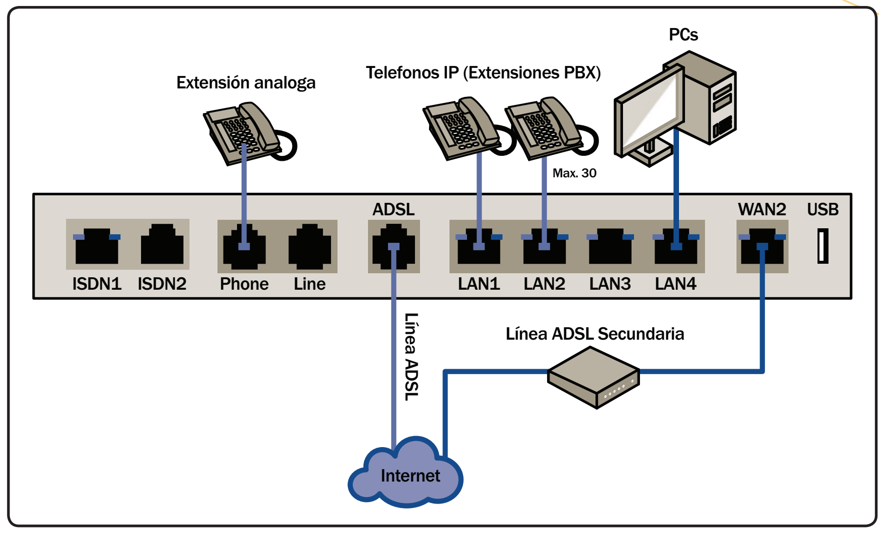


Figura 12. Para evitar problemas de funcionamiento en la conexión VoIP debemos verificar la adecuada conexión de cada medio.

Redes **empresariales**

Los diferentes departamentos de una empresa representan el área de trabajo al que nos hemos referido a lo largo del capítulo. Una red organizativa, por lo general, se encuentra segmentada según el número de departamentos de la compañía. De la misma manera, los nodos están distribuidos en los diferentes pisos, edificios o sucursales (de diferentes países).

Los hoteles, los bancos y las oficinas de atención a clientes son ejemplos de empresas que mantienen distribuidos sus equipos en áreas de trabajo, pero que poseen una única sala de telecomunicaciones, que no se encuentra a la vista de los usuarios.



SOLUCIONES VOIP

Avanvox es el nombre de una centralita IP que utiliza la tecnología open source Asterisk. Por lo general, este recurso hace uso de un servidor de fax basado en Hylaf. Para obtener más detalles, consultar: www.voip.ms.

La mayoría de las empresas modernas cuentan con más de una sucursal, lo que involucra un espacio considerable y un enlace troncal de mayor cobertura. Las redes inalámbricas han sido una opción para ellas, porque permiten comunicar a distancia un área con otra en diferente espacio geográfico, aunque no siempre su enlace satelital es óptimo y ciento por ciento inmune a fallas.



RESUMEN

En este capítulo analizamos las condiciones ambientales de un cuarto de telecomunicaciones y algunos aspectos que deben considerarse en el diseño de las áreas de trabajo. También vimos algunos detalles sobre la instalación de recursos VoIP en una red informática.



Capítulo 6

Seguridad en la red empresarial

Conoceremos algunas herramientas y consejos para mantener la seguridad en una red empresarial.



Introducción

Las redes implementadas en pequeñas y medianas empresas suelen tener una mayor cantidad de medidas de seguridad en comparación con las redes hogareñas o de oficina. Esto se debe, desde luego, al tamaño, que implica que la red empresarial sea más robusta y, además, a que los usuarios (con sus necesidades y exigencias), por la tarea que realizan, son muy demandantes en este sector. Por lo tanto, es necesario tener presente que no es lo mismo, por ejemplo, monitorear la red de un cibercafé que la de una compañía en su totalidad.

ARQUITECTURA CLIENTE-SERVIDOR

Como consecuencia de lo anteriormente mencionado, es importante destacar que en ciertas compañías es cada vez más común la adopción de la **arquitectura cliente-servidor**. Esta consiste en un modelo de aplicación distribuida compuesta por un conjunto de equipos que, a menudo, solicitan servicios y recursos a una computadora en particular (o a un conjunto de computadoras, en algunos casos), llamada servidor o server. Esta arquitectura es muy propensa a sufrir problemas, sobre todo, si el sistema operativo del servidor no está bien configurado y trabajando en óptimas condiciones.

Windows

Se sabe que Windows es uno de los sistemas operativos más utilizados en el mundo. Su versión varía de acuerdo con su uso o explotación, y con frecuencia es usado por millones de usuarios o clientes que dependen de una alta gama de recursos físicos y lógicos.

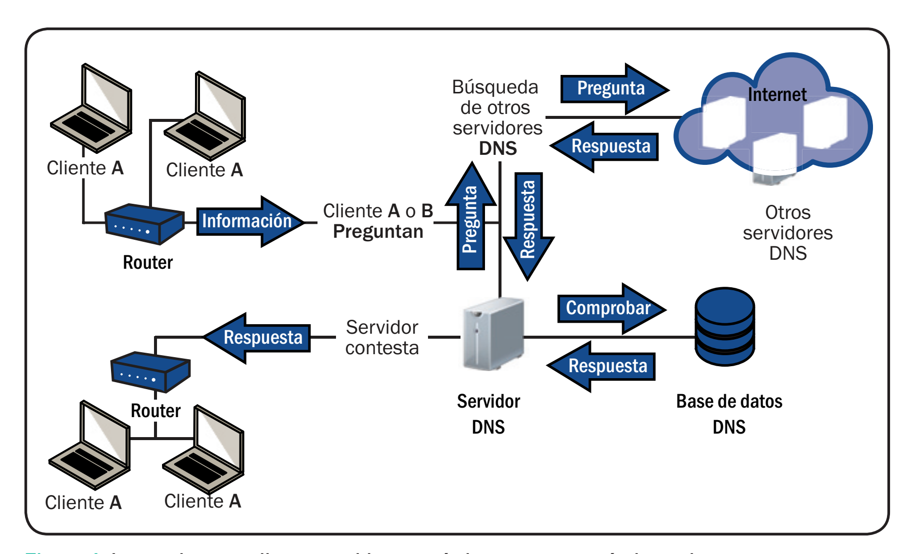


Figura 1. La arquitectura cliente-servidor es prácticamente un estándar en la empresa.



Figura 2. Desde la página de Ubuntu, **se puede adquirir la versión** Server **para la red.**

La presencia de **Windows 7** y **Windows 8** representa, hoy en día, un estándar para los equipos cliente, mientras que **Windows 2008 Server** y **Windows 2012 Server** lo son para equipos servidores. Más adelante abordaremos algunos aspectos de la configuración para delegar funciones administrativas a una red corporativa desde un sistema operativo Windows 2008 Server.

GNU-Linux

Existen otros sistemas operativos alternativos al diseñado por Microsoft. **GNU-Linux** también se caracteriza por estar presente en millones de computadoras. En la actualidad, se encuentra instalado no solo en plataformas PC, sino también en diversas gamas de dispositivos móviles (teléfonos celulares y tabletas PC).

Esta es una opción muy interesante de libre distribución, que puede convertirse en la mejor herramienta para llevar la administración de una compañía. Algunas distribuciones comerciales, como Ubuntu de Canonical, integran una versión de su sistema para clientes y otra distinta para servidores.

Recientemente, se ha dado a conocer una fusión entre dos grandes empresas del mundo del desarrollo y la tecnología: Canonical y Dell. Ambas se unieron para ofrecer una amplia gama de configuraciones de equipos informáticos, entre los que destacan los servidores.

Los servidores **PowerEdge 10G**, **11G** y **12G** de **Dell** están certificados con **Ubuntu 12.04 LTS**



UN KERNEL MUY SEGURO

El kernel del sistema operativo GNU/Linux cuenta con niveles de seguridad más potentes que el desarrollado por Microsoft. Esto lo convierte en un sistema con mayor estabilidad y menos vulnerable. GNU/Linux es distribuido en toda Europa.



Figura 3. Sevidor PowerEdge 12G **lanzado conjuntamente por** Dell **y** Canonical.

(GNU-Linux) y ofrecen a los clientes una gran variedad de dispositivos de alto rendimiento.

LAS REDES EN PRIMER PLANO

Actualmente, las tecnologías de la información y las comunicaciones (TIC) han hecho posible el crecimiento de las redes y, también, su transformación; las ha posicionado en el mercado informático como una fuente de desempeño y producción ineludible. Quizás esta sea la razón por la que la empresa moderna tiene la necesidad de implementar soluciones tecnológicas centradas en el mundo de la redes.

Las principales soluciones tecnológicas implementadas en una empresa, por lo general, apuestan a la seguridad (aunque este no sea el principal objetivo de la organización). Por lo tanto, deben implementarse medidas que funcionen como herramientas efectivas en contra de diversos ataques.

Una solución informática a nivel de la seguridad que no puede faltar en ninguna red empresarial es el **monitoreo**. A menudo, este se puede llevar a cabo de manera remota, desde un servidor o desde cualquier equipo conectado a la red, con solo conocer datos como la



Figura 4. La conexión remota representa una puesta en práctica del monitoreo.

dirección IP y el grupo de trabajo o dominio. Si bien en capítulos anteriores hemos tratado este tema, más adelante explicaremos cómo realizar esta tarea con la ayuda de una herramienta de Windows conocida como **Conexión a escritorio remoto**.

POLÍTICAS DE SEGURIDAD

Para implementar una arquitectura cliente-servidor, se ha definido una serie de **políticas de seguridad** que debemos cumplir. Una buena elección de estas políticas evitará **problemas de vulnerabilidad en los accesos** y **en la seguridad de la integridad de los recursos**.

Las políticas de seguridad consisten en un conjunto de reglas que, por lo general, se establecen tanto a **nivel usuario** como a **nivel recursos** (equipos). En el primer caso, estas políticas tienen como finalidad restringir accesos, controlar la instalación indebida de programas y evitar los cambios en la configuración. Para el caso de los equipos, las reglas consisten en estandarizar sus propiedades, las configuraciones y los permisos.

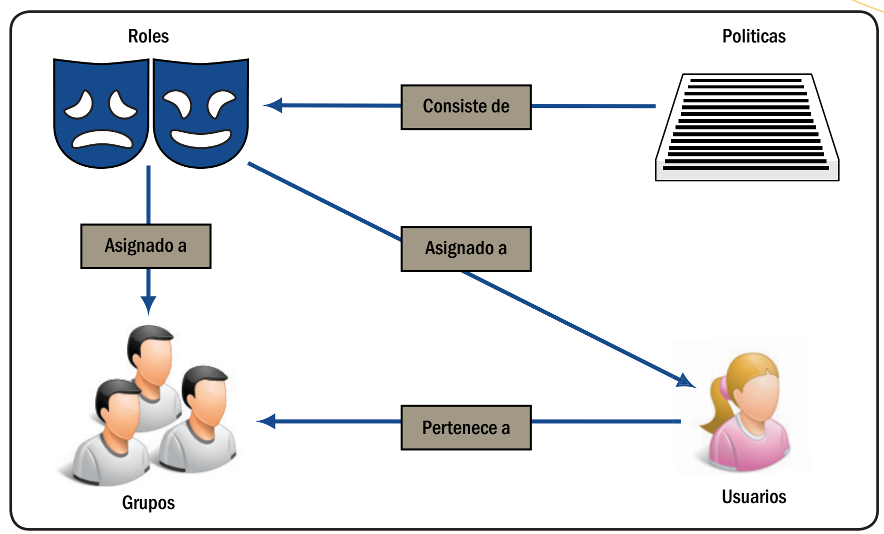


Figura 5. Esquema de gestión de políticas de seguridad en una empresa.

En el último apartado de este capítulo describiremos el entorno para la administración de políticas de grupo desde Windows 2008 Server. Esto nos permitirá tener una idea más certera de las políticas de seguridad aplicadas en una empresa.

Monitoreo del área de trabajo

El monitoreo es un sistema de rastreo, verificación y supervisión de los procesos informáticos, tanto físicos como lógicos. Puede llevarse a cabo mediante herramientas de software o hardware, según la necesidad de la empresa, y se realiza con el objetivo de mantener segura el área de trabajo.

Con el crecimiento de la tecnología, muchas compañías recurren frecuentemente a este tipo de servicio, cuya implementación se logra a través de la explotación de recursos presentes en sus redes de datos.

La tarea de monitoreo tiene como finalidad reflejar un determinado estado o historial de los problemas ocurridos en la infraestructura del entorno de trabajo, con la intención de cubrir ciertas vulnerabilidades, alimentar diversos **procesos IT** e implementar un cúmulo de contramedidas:

- Gestión de fallas
- Gestión de incidentes
- Gestión de rendimiento
- Gestión de capacidad (administración o planificación)



Figura 6. Las cámaras IP **utilizan el protocolo de Internet para funcionar en la red.**

La seguridad física y lógica en las empresas es muy importante, motivo por el cual existen diversos tipos de monitoreo, que van desde los manuales hasta los virtuales. En la próxima sección, describiremos los clases de monitoreo bajo soluciones IT (redes de datos) más comunes en las empresas.

En la actualidad, muchas compañías dedican un área especial para el monitoreo de áreas de trabajo y determinados procesos. Estos entornos van conectados directamente a diversas centrales o cuartos de telecomunicaciones mediante un **enlace IT**. El monitoreo se hace en tiempo real a través de la red de datos de la organización. Esto se logra gracias al protocolo de Internet y al uso de cámaras especiales, más conocidas como **cámaras IP**.

TIPOS DE MONITOREO

Los tipos de monitoreo informático pueden variar de acuerdo con la necesidad de cada compañía, por lo que siempre es importante considerar algunos aspectos técnicos antes de adquirir un sistema de esta clase:

- El ahorro de tiempo que la herramienta brinda por la automatización de controles que permite realizar debe ser significativamente mayor que el tiempo de administración demandado por la herramienta.
- La herramienta debe permitirnos un ahorro de tiempo en capacitación de personal.
- Facilidad y rapidez en la emisión de reportes (**reporting**) por parte de la herramienta.
- Permiso para acceder desde otras aplicaciones o dispositivos de la red. -
- Posibilidad de darles privilegios de rastreo a los distintos actores para facilitar el ingreso del producto a la empresa.
- Contar con un **overview** de la disponibilidad del servicio o de ciertos parámetros.



LAS CÁMARAS IP

Las cámaras IP modernas integran aplicaciones para la detección de presencia, la grabación de imágenes o las secuencias en equipos informáticos. Son muy demandadas por muchas empresas. Algunas marcas comerciales son: Geovision, Panasonic y Vivotek.



Figura 7. NoxGlobe **es una solución para el monitoreo de una compañía.**

- Contar con alternativas de notificaciones (independientes de la presencia del personal).
- Disponer de alarmas en tiempo real.

Una vez elegido el producto adecuado para la empresa, recomendamos probar la solución en forma inmediata, para descartar la posibilidad de dañar algún recurso propio de la compañía. NoxGlobe es una opción interesante que cuenta con las características antes mencionadas. Para obtener mayor información sobre el producto, recomendamos consultar el sitio www.noxglobe.com.

En la Tabla 1 describimos las distintas clases de monitoreo más frecuentemente utilizadas por las compañías.

TIPOS DE MONITOREO

CLASE	DESCRIPCIÓN
Manual	Es el más común. El técnico se encarga de revisar los parámetros relevantes de la estructura IT para la detección de problemas que se resolverán con posterioridad.
Automático	El monitoreo se realiza mediante sistemas de control informáticos y planificadores.
Local	Involucra recursos del equipo por monitorear, centrándose en una inspección física de la estructura de la compañía.
Remoto	Se lleva a cabo sin utilizar recursos del equipamiento monitoreado. A menudo, es a distancia.

Tabla 1. **Diferentes monitoreos aplicados en las empresas.**

El monitoreo remoto

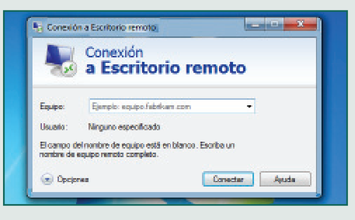
El monitoreo remoto, por lo general, se realiza a distancia y sin utilizar recursos del equipo por monitorear. En este caso, veremos cómo efectuar una conexión remota desde un sistema operativo Windows.

La **conexión al escritorio remoto** es una de las opciones de comunicación remota que poseen los sistemas operativos modernos de cualquier computadora. Se trata, básicamente, de una interfaz de software que nos permite monitorear otros equipos conectados a la red de una compañía.

Para conectarse a un equipo remoto, es necesario que la computadora a la cual nos comunicaremos esté encendida, tener una conexión de red, habilitar el escritorio remoto y tener permisos de conexión (establecidos por el administrador de la red). Luego, debemos realizar los siguientes pasos:

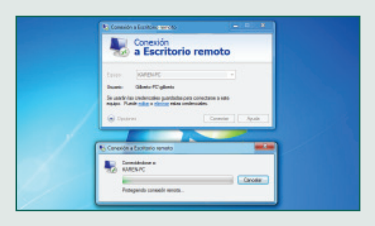
PASO A PASO /1
Preparar el acceso remoto de Windows

1



Para abrir la **Conexión al escritorio remoto**, haga clic en el botón **Iniciar** y, en el cuadro de búsqueda, escriba el comando **mstsc**. Aparecerá una ventana que solicita el **nombre del equipo** al que quiere conectarse.

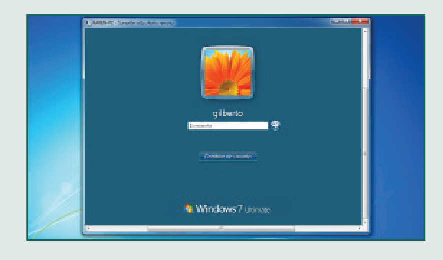
2



Ingrese el nombre completo del equipo remoto. Una manera de conocerlo es a través de las **Propiedades** del equipo. Oprima el botón **Conectar**. El sistema intentará comunicarse con el equipo remoto.

PASO A PASO /1 (cont.)





Una vez que se establece la conexión, aparece una nueva ventana que solicita la **clave** del equipo anfitrión. Ingrésela y pulse **Aceptar**. Se abrirá el escritorio del equipo remoto.

Otras opciones interesantes para el monitoreo remoto son **VNC**, **NetSupport** y **TeamViewer**. Estas herramientas, por lo general, pueden descargarse de Internet.

Resguardo y protección de la información

Los discos duros externos, las memorias USB, los discos compactos y otros dispositivos de almacenamiento son, sin duda, los recursos más utilizados por los usuarios para resguardar los millones de datos que residen en su computadora. Sin embargo, no son los únicos medios que nos permiten hacer esa tarea.

Actualmente, también disponemos de **cloud computing** o computación en la nube.

La computación en la nube integra múltiples servicios y aplicaciones de seguridad (escáner, antivirus), almacenamiento, entretenimiento, descargas, recursos educativos, etc. Por ejemplo, si deseamos conocer el estado de seguridad de una computadora o de una red completa, podemos utilizar un escáner online.

Los sitios web para el almacenamiento e intercambio de archivos, denominados **Cloud Storage**, forman parte también de lo que hoy llamamos computación en la nube. Este servicio les ofrece a los usuarios individuales y a las empresas una forma segura de almacenamiento de datos con fines de resguardo. Pero también existen compañías que apuestan a

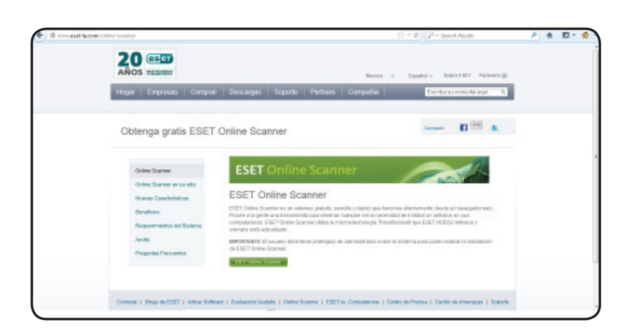


Figura 8. Los escáneres online forman parte de las soluciones de cloud computing.

infraestructuras que incluyen un plan de escalabilidad, cobertura, mayor potencia y seguridad en el proceso del sostén de su información.

Candados de seguridad

En capítulos anteriores, hablamos sobre la importancia de proteger una red informática y, específicamente, sobre los accesos no autorizados.

Los métodos que tienen como objetivo frenar el paso de las amenazas en una organización y restringir ciertos privilegios se llaman **candados de seguridad**.

Es probable que, en más de una oportunidad, nos hayamos preguntado: ¿cómo restringir ciertos sitios de Internet para evitar

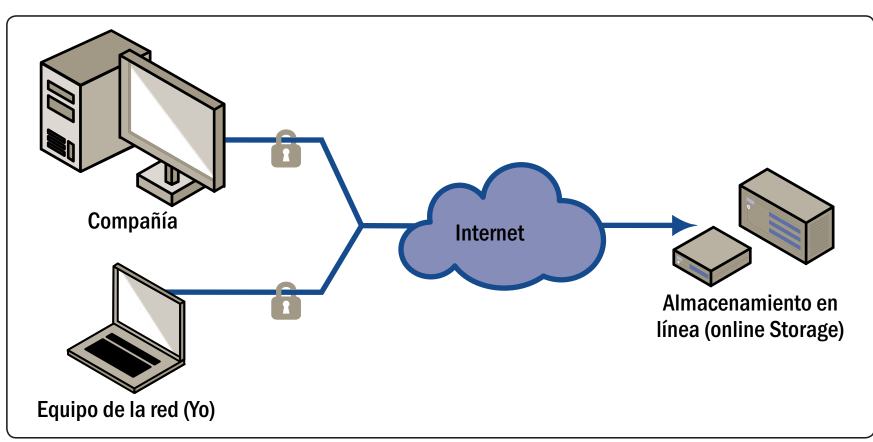
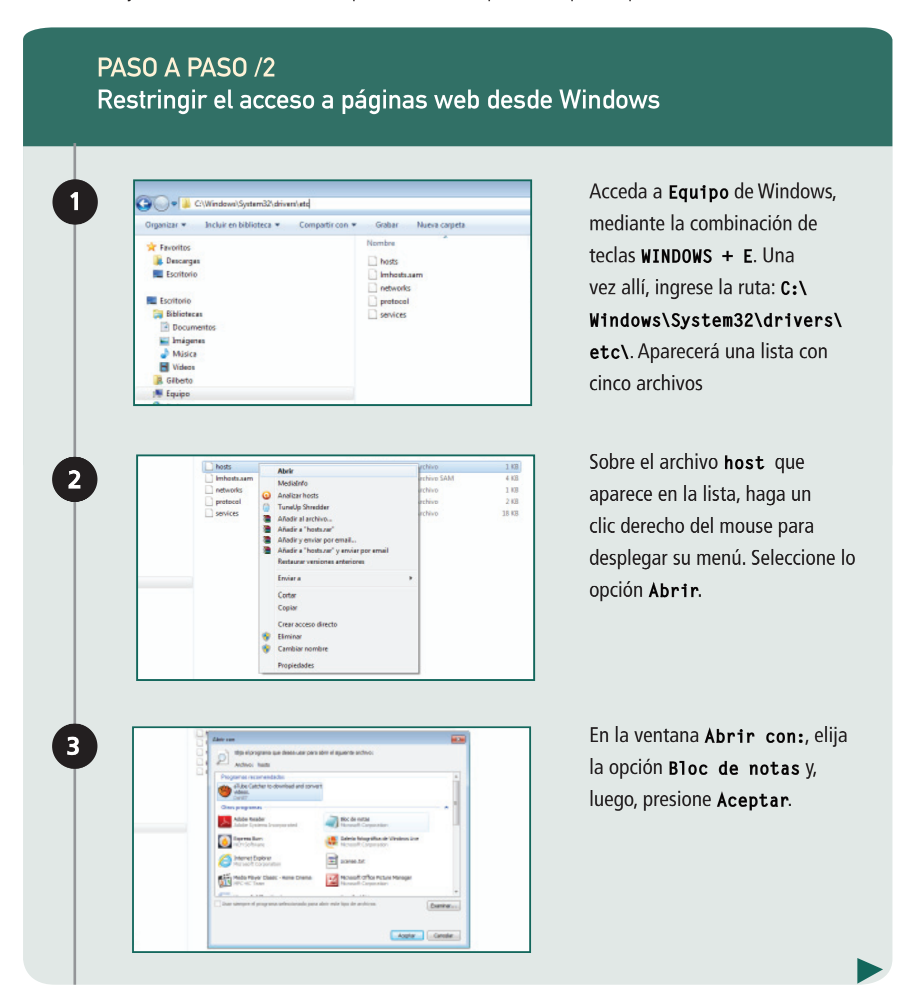


Figura 9. Distribución de los recursos de una red bajo una infraestructura Cloud Storage.

que los usuarios tengan acceso a sus recursos? Sabemos que no todas las páginas web son permitidas en algunas compañías, con la intención de evitar el malware proveniente de Internet y la distracción de los empleados.

En el siguiente **Paso a Paso** aprenderemos a restringir el acceso a las páginas de Internet desde el sistema operativo Windows. Veremos que es un procedimiento muy simple, que requiere de pocos pasos.



PASO A PASO /2
Restringir el acceso a páginas web desde Windows

1 Acceda a **Equipo** de Windows, mediante la combinación de teclas **WINDOWS + E**. Una vez allí, ingrese la ruta: **C:\Windows\System32\drivers\etc**. Aparecerá una lista con cinco archivos

2 Sobre el archivo **host** que aparece en la lista, haga un clic derecho del mouse para desplegar su menú. Seleccione la opción **Abrir**.

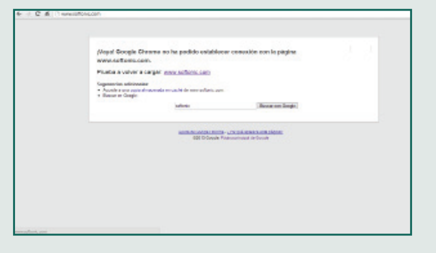
3 En la ventana **Abrir con:**, elija la opción **Bloc de notas** y, luego, presione **Aceptar**.

PASO A PASO /2 (cont.)



Para restringir un sitio web, ingrese la dirección IP del servidor, acompañada del nombre del sitio, como se muestra en la parte inferior de la imagen. Para terminar, cierre la ventana y guarde los cambios.





Para comprobar que la configuración ha tenido éxito, abra el navegador e intente acceder al sitio bloqueado. Aparecerá un mensaje que informa que no es posible establecer conexión con la página solicitada.

Desde el S.O.

Windows 2008 Server contiene la herramienta **Group Policy Management Console**, que facilita la administración de grupos para hacer funcionar un sistema de una empresa. En el siguiente **Paso a Paso** explicamos cómo habilitar la **Administración de directivas de grupo**, desde Windows 2008 Server.

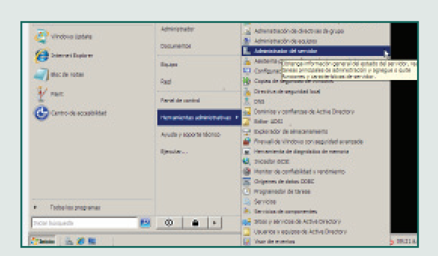


SITIOS DE CLOUD COMPUTING

EyeOS **es un sitio de Internet que ofrece aplicaciones y servicios de cloud computing para la pequeña y mediana empresa. Este sitio es usado por IBM, NEC, Unisys, Mitsubishi Electric, etc. Para mayor información, visitar: www.eyeOS.com.**

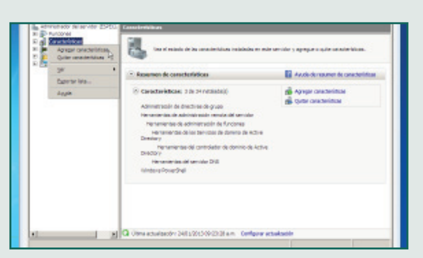
PASO A PASO /3
Directivas de grupo desde Windows 2008 Server

1



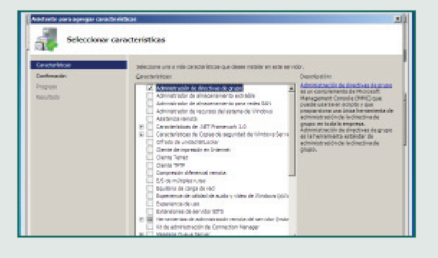
Para conectarse al equipo controlador de dominio (Active Directory), vaya a **Inicio/Herramientas administrativas/ Administración del servidor**.

2



Para continuar, pulse el botón secundario del mouse sobre la opción **Características** del árbol de la derecha y elija la opción **Agregar características**.

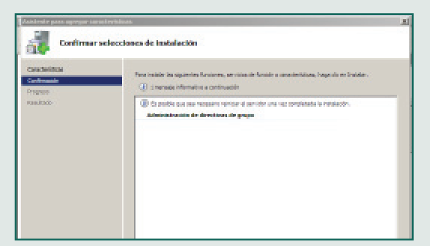
3



Marque la casilla de verificación de la opción **Administración de directivas de grupo**. Esto le permitirá agregar una nueva función al servidor, para facilitarle la administración de políticas del dominio. Pulse **Siguiente**.

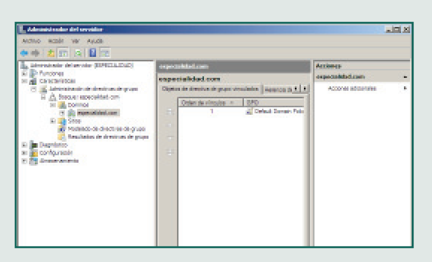
PASO A PASO /3 (cont.)





En la nueva ventana, presione **Instalar**. Comenzará la instalación de la característica elegida. Espere unos minutos.





En la ventana **Administración del servidor** verifique que la característica anterior ya haya sido dada de alta.



RESUMEN

En este capítulo analizamos aspectos importantes para preservar la seguridad en la red de una empresa. Hicimos un recorrido por la arquitectura cliente-servidor, el monitoreo, cloud computing, cloud storage y tareas sencillas de configuración sobre sistemas Windows (Seven y 2008 Server).

Técnico en REDES & SEGURIDAD

